CENTRE FOR INFORMATION TECHNOLOGY

Research Project– INFO901

The recommended cybersecurity practices for Facebook users from users' point of view

Submitted to

Dr Monjur Ahmed

Dr Prashant Khanna

Submitted by

Name: Thilini Bhagya Gothami Herath

ID: 19488886

Statement of Authenticity

By submitting this work, I declare that this work is entirely my own except those parts duly identified and referenced in my submission. It complies with any specified word limits and the requirements and regulations detailed in the coursework instructions and any other relevant program module declaration. In submitting this work, I acknowledge that I have read and understood the regulations and code regarding academic misconduct, including that relating to plagiarism, as specified in the program handbook. I also acknowledge that this work will be subject to a variety of checks for academic integrity.

Acknowledgment

I wish to convey my sincere gratitude to Dr Monjur Ahmed (principal supervisor) and Dr Prashant Khanna (Secondary supervisor) for guiding me and providing valuable comments throughout my research work.

Also, I would like to express my sincere gratitude to Dr Kay Fielden for her immense support in preparing the research proposal last semester.

Then I would like to thank Dr Guss Wilkinson for providing me the opportunity to take part in this research.

Next, my heartfelt thank goes to Human Ethics in Research Group (HERG) of Waikato Institute of Technology (Wintec) and especially to Megan Allardice for her immense support in approving my research proposal within a minimum timeframe.

Last but not least I would like to thank all my family members back in Sri Lanka as well as my friends in New Zealand and Sri Lanka who have supported me immensely for the successful completion of my research work.

Abstract

Background:	The vulnerability of Facebook users grows day by day since cyber threats against Facebook users emerge accordingly. Therefore the cybersecurity and cyber behavior play a vital role when safeguarding the privacy of Facebook users.
Purpose :	Identifying the recommended best practices for Facebook users in New Zealand and Sri Lanka.
Method and Methodology:	The post-positivist method with quantitative methodology is used when conducting the research
Findings :	The researcher found that age, gender, and education levels have 80%, 20%, and 40% impact on cyber awareness respectively. Also, it is found that there is a 100% impact from user's cyber awareness to user's cyber behavior. The impact of cyber behavior on the vulnerability level of Facebook users is revealed as 66.67%. The research also revealed that even a small portion of all age, gender groups, and education levels are vulnerable to cyber threats.
Conclusion:	This research paper and its findings are significant for individual Facebook users as well as for employers who look forward to improving their employees' cybersecurity awareness and cyber behavior.

Keywords: *Cybersecurity Awareness, Cybersecurity Behavior, Facebook Users, Recommended practices*

Table of Contents

1. Introduction 1

1.1 Background 1
1.2 Problem Statement 2
1.3 Research Objectives 3
1.4 Research Contribution 3
1.5 High-level Structure of Overall Research Report 4
1.6 Conclusion 4

2. Literature Review 5

2.1 PRISMA Statement 5
2.2 Literature Theme and Sub-theme 8
2.2.1 Cyberthreats on the Internet 9
2.2.2 Cybersecurity on the Internet 14
2.2.3 Cybersecurity on Social Media 22
2.3 Research questions 32
2.4 Conclusion 33

3. Research Method 34

3.1 Research Questions and Hypotheses 34
3.2 Research Design 38
3.3 Research Instrument 40
3.4 Sample Size 40
3.5 Sample Method 42
3.6 Data Collection 42
3.7 Primary Data Description 42
3.8 Data Analysis Method 43
3.8.1 Raw Data 43
3.8.2 Editing 43
3.8.3 Coding 43
3.8.4 Cronbach's Alpha 44
3.8.5 Descriptive Analysis 44
3.8.6 Univariate Analysis: Chi-square 44
3.8.7 Bivariate Analysis: ANOVA 52
3.9 Limitations of the Methodology 53
3.10 Conclusion 53

4. Results 54
4.1 Introduction 54
4.2 Data Analysis 54
4.2.1 Cronbach's Alpha 54
4.2.2 Descriptive Analysis 55
4.2.3 Univariate Analysis: Chi-Square 67
4.2.4 Bivariate Analysis: ANOVA 104
4.2.5 Conclusion 109
5. Discussion 110
5.1 Introduction 110
5.2 Discussion on Descriptive Analysis 110
5.3 Discussion on Chi-square Analysis 123
5.4 Discussion on ANOVA Analysis 132
5.5 Recommended Practices for Facebook Users 132
5.6 Conclusion 136
6. Conclusion 137
6.1 Limitations 137
6.2 Future Work 137
6.3 Concluding Remarks 138
References 139
Appendix A – Survey Questions 145
Appendix B – Coding Structure Used in SPSS 149
Appendix C – Descriptive Analysis with Stacked Bar Charts 154
Appendix D-Ethics form 190

List of Tables

Table 2.1: PRISMA statement's inclusion and exclusion criteria…….6

Table 2.2.1 Theme article table: Cyberthreats on the internet……...9

Table 2.2.1.1 Theme article table: Cyberthreats in Social Media……11

Table 2.2.2 Theme article table: Cybersecurity on the Internet……...14

Table 2.2.2.1 Theme article table: User Awareness When Using the Internet……16

Table 2.2.2.2 Theme article table: User Behavior When Using the Internet…….…..18

Table 2.2.3 Theme article table: Cybersecurity on Social Media……....23

Table 2.2.3.1 Theme article table: User Awareness When Using Social Media…….…25

Table 2.2.3.1.1 Theme article table: User Awareness When Using Facebook…….…...26

Table 2.2.3.2 Theme article table: User Behavior When Using Social Media……....28

Table 2.2.3.2.1 Theme article table: User Behavior When Using Facebook……...30

Table 3.1 Connection between Main RQ, Literature review, Hypotheses, Sub-research questions, and survey questions ……..……40

Table 3.2 New Zealand's age and gender-wise Facebook user distribution (Source: NapoleonCat, 2021) ……....40

Table 3.3 Sri Lanka's age and gender-wise Facebook user distribution (Source: NapoleonCat, 2021) …….…..41

Table 3.4 Age, relevant survey questions and related hypotheses for chi-square analysis ….45

Table 3.5 Gender, relevant survey questions and related hypotheses for chi-square analysis…….46

Table 3.6 Education Level, relevant survey questions and related hypotheses for chi-square analysis……...……..47

Table 3.7 Cyber awareness, Cyber behavior, relevant survey questions and related hypotheses for chi-square analysis …… 48

Table 3.8 Cyber behavior, relevant survey questions and related hypotheses for chi-square analysis ……....49

Table 3.9 Independent variables, relevant survey questions and related hypotheses for ANOVA test ……52

Table 4.1 Case processing summary …….…..54

Table 4.2 Cronbach's alpha result……55

Table 4.3 Age-wise distribution of survey participants …….….55

Table 4.4 Gender wise distribution of survey participants ……..56
Table 4.5 Education level-wise distribution of survey participants ……....57
Table 4.6 Time spent on Facebook ……58
Table 4.7 Awareness of creating a strong password ……..……..58
Table 4.8 Follow instructions when creating the password…….……59
Table 4.9 Awareness of personal information disclosure in profile……...…….59
Table 4.10 Current view of email/telephone number/address in the profile……60
Table 4.11 Awareness of two-factor authentication ……....60
Table 4.12 Use of two-factor authentication ……...61
Table 4.13 Awareness of setting up who can send friend requests…….….61
Table 4.14 Use of setting up who can send friend requests feature…….61
Table 4.15 Check and update the privacy and security settings…….…..62
Table 4.16 Accept friend requests……....62
Table 4.17 Send friend requests……..….63
Table 4.18 Clicking unknown links…….63
Table 4.19 Password change frequency on Facebook…….……64
Table 4.20 Logging out from devices after using Facebook……...64
Table 4.21 Consideration of security before sharing photos, videos, and posts on Facebook……..65
Table 4.22 Current view photos, videos, and posts on Facebook……65
Table 4.23 Current view photos, videos, and posts on Facebook……66
Table 4.24 Current view photos, videos, and posts on Facebook……....66
Table 4.25 Number of respondents answered to SQ5……..67
Table 4.26 Cross-tabulation Age * SQ5……...…67
Table 4.27 Chi-square result for Age * SQ5……68
Table 4.28 Number of respondents answered to SQ7…….….68
Table 4.29 Cross-tabulation Age * SQ7…….……..69
Table 4.30 Chi-square result for Age * SQ7……69
Table 4.31 Number of respondents answered to SQ9…….……70
Table 4.32 Cross-tabulation Age * SQ9……...70
Table 4.33 Chi-square result for Age * SQ9……...….70

Table 4.34 Number of respondents answered to SQ11……71
Table 4.35 Cross-tabulation Age * SQ11…….....71
Table 4.36 Chi-square result for Age * SQ11……..…71
Table 4.37 Number of respondents answered to SQ19……72
Table 4.38 Cross-tabulation Age * SQ19……...…….72
Table 4.39 Chi-square result for Age * SQ19…….……72
Table 4.40 Number of respondents answered to SQ5…….…….73
Table 4.41 Cross-tabulation Gender * SQ5……..……73
Table 4.42 Chi-square result for Gender * SQ5……...73
Table 4.43 Number of respondents answered to SQ7……..……74
Table 4.44 Cross-tabulation Gender * SQ7…….…….74
Table 4.45 Chi-square result for Gender * SQ7…….……..74
Table 4.46 Number of respondents answered to SQ9……..75
Table 4.47 Cross-tabulation Gender * SQ9…….…….75
Table 4.48 Chi-square result for Gender * SQ9……..…….75
Table 4.49 Number of respondents answered to SQ11…….…….……..76
Table 4.50 Cross-tabulation Age * SQ11……76
Table 4.51 Chi-square result for Age * SQ11……..76
Table 4.52 Number of respondents answered to SQ19……...…….77
Table 4.53 Cross-tabulation Gender * SQ19……...77
Table 4.54 Chi-square result for Gender * SQ19……77
Table 4.55 Number of respondents answered to SQ5……..78
Table 4.56 Cross-tabulation Education level * SQ5……78
Table 4.57 Chi-square result for Education level * SQ5……..78
Table 4.58 Number of respondents answered to SQ7……..79
Table 4.59 Cross-tabulation Education level * SQ7……79
Table 4.60 Chi-square result for Education level * SQ7……..80
Table 4.61 Number of respondents answered to SQ9…….….80
Table 4.62 Cross-tabulation Education level * SQ9……...…80
Table 4.63 Chi-square result for Education level * SQ9……..…81

Table 4.64 Number of respondents answered to SQ11……81
Table 4.65 Cross-tabulation Education level * SQ11……..81
Table 4.66 Chi-square result for Education level * SQ11……82
Table 4.67 Number of respondents answered to SQ19……....82
Table 4.68 Cross-tabulation Education level * SQ19……..83
Table 4.69 Chi-square result for Education level * SQ19……...…83
Table 4.70 Number of respondents answered to SQ5 and SQ6……..…….84
Table 4.71 Cross-tabulation actual awareness (SQ5) * actual behavior (SQ6)……..…..……84
Table 4.72 Chi-square result for actual awareness (SQ5) * actual behavior (SQ6)……....84
Table 4.73 Number of respondents answered to SQ7 and SQ8……...85
Table 4.74 Cross-tabulation actual awareness (SQ7) * actual behavior (SQ8)……...85
Table 4.75 Chi-square result for actual awareness (SQ7) * actual behavior (SQ8)……..…86
Table 4.76 Number of respondents answered to SQ9 and SQ10…….86
Table 4.77 Cross-tabulation actual awareness (SQ9) * actual behavior (SQ10)…….86
Table 4.78 Chi-square result for actual awareness (SQ9) * actual behavior (SQ10)……...87
Table 4.79 Number of respondents answered to SQ11 and SQ12……...87
Table 4.80 Cross-tabulation actual awareness (SQ11) * actual behavior (SQ12)……...……87
Table 4.81 Chi-square result for actual awareness (SQ11) * actual behavior (SQ12)……88
Table 4.82 Cross-tabulation actual awareness (SQ19) * actual behavior (SQ20)……...88
Table 4.83 Chi-square result for actual awareness (SQ19) * actual behavior (SQ20)…….88
Table 4.84 Number of respondents answered to SQ4……..89
Table 4.85 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ4)…...89
Table 4.86 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ4).....89
Table 4.87 Number of respondents answered to SQ6…….……90
Table 4.88 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ6)…...90
Table 4.89 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ6)……91
Table 4.90 Number of respondents answered to SQ8……..……91
Table 4.91 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ8)…...92

Table 4.92 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ8)……92
Table 4.93 Number of respondents answered to SQ10……...…….93
Table 4.94 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ10)….93
Table 4.95 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ10)……..93
Table 4.96 Number of respondents answered to SQ12……94
Table 4.97 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ12)….94
Table 4.98 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ12)…….….94
Table 4.99 Number of respondents answered to SQ13……...…….95
Table 4.100 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ13)……..95
Table 4.101 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ13)…….….96
Table 4.102 Number of respondents answered to SQ14…….……96
Table 4.103 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ14)……..97
Table 4.104 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ14)……..97
Table 4.105 Number of respondents answered to SQ15…….……98
Table 4.106 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ15)……..98
Table 4.107 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ15)……..98
Table 4.108 Number of respondents answered to SQ16…….……....99
Table 4.109 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ16)……..…....99
Table 4.110 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ16)…….……...100
Table 4.111 Number of respondents answered to SQ17……100
Table 4.112 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ17)……101

Table 4.113 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ17)……...101
Table 4.114 Number of respondents answered to SQ18……...102
Table 4.115 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ18)……102
Table 4.116 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ18)……102
Table 4.117 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ20)……...103
Table 4.118 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ20)……103
Table 4.119 Age * Gender* Education level-wise respondents distribution……...104
Table 4.120 ANOVA results for Age * Gender* Education level for SQ5.....105
Table 4.121 ANOVA results for Age * Gender* Education level for SQ7……...106
Table 4.122 ANOVA results for Age * Gender* Education level for SQ9……...107
Table 4.123 ANOVA results for Age * Gender* Education level for SQ11……108
Table 4.124 ANOVA results for Age * Gender* Education level for SQ19……109
Table 5.1: Findings of descriptive analysis results related to age-wise awareness of users……...110
Table 5.2 Findings of descriptive analysis results related to gender-wise awareness of users …….....112
Table 5.3 Findings of descriptive analysis results related to education level-wise awareness of users ……114
Table 5.4 Findings of descriptive analysis results related to actual cyber awareness vs. actual cyber behavior……...117
Table 5.5 Findings of chi-square test analysis results related to age…….....123
Table 5.6 Age-wise respondent distribution and cyber awareness……...124
Table 5.7 Findings of chi-square test analysis results related to gender …….....125
Table 5.8 Gender-wise respondent distribution and cyber awareness …….....126
Table 5.9 Findings of chi-square test analysis results related to education level…….....126
Table 5.10 Education level-wise respondent distribution and cyber awareness……....127
Table 5.11 Findings of chi-square test analysis results related to cyber awareness …….....128

Table 5.12 Findings of chi-square test analysis results for believed cyber awareness over vulnerability level of the Facebook users ……..…….....129
Table 5.13 Findings on overall ANOVA analysis ……...…….132
Table 5.14 Age wise recommended practices for Facebook users ……...133
Table 5.15 Gender wise recommended practices for Facebook users ……..134
Table 5.16 Education level-wise recommended practices for Facebook users……...…..134

List of Figures

Figure 1.1: Outline of the research report 4
Figure 2.1: PRISMA flow chart 7
Figure 2.2: Concept map 8
Figure 3.1: Four world views (Creswell & Creswell, 2018) 34
Figure 3.2: Modified UTAUT Model 39
Figure 3.3: Connection between variables, LR, H, and RQ in the modified UTAUT model 39
Figure 3.4: Sample size (source: Creative Research Systems, 2021) 41
Figure 3.5: Overview of the Stages of Data Analysis (Sonquist & Dunkelberg, 1977; as Zikmund, Babin, Carr cited by, & Giffin, 2013) 43
Figure 3.6 Chi-square category variables: Age and other survey questions 45
Figure 3.7: Chi-square category variables: Gender and other survey questions 45
Figure 3.8: Chi-square category variables: Education level and other survey questions 46
Figure 3.9 Chi-square category variables: cyber awareness, cyber behavior, and other survey question 47
Figure 3.10: Chi-square category variables: cyber behavior and other survey questions 49
Figure 3.11: ANOVA test age * gender* education level for main survey questions 52
Figure 4.1: Age-wise distribution of survey participants 55
Figure 4.2: Gender wise distribution of survey participants 56
Figure 4.3: Education level-wise distribution of survey participants 57
Figure 5.1: Impact of cyber awareness over cyber behavior as per discussion on descriptive analysis 120
Figure 5.2: Impact of cyber behavior over vulnerability level of Facebook users 122
Figure 5.3: Modified UTAUT Model 123
Figure 5.4: Modified UTAUT Model with proved hypotheses 131

1. Introduction

Many cyber threats are blooming on social media platforms nowadays such as identity theft, spam attacks, malware attacks, Sybil attacks, social phishing, impersonation, hijacking, fake requests, and image retrieval and analysis (Zhang & Gupta, 2018). Therefore, proper user cyber awareness and cyber behavior are crucial in social networking sites to minimize user vulnerabilities. This research is primarily focusing on identifying recommended practices for Facebook users from the user's point of view in New Zealand and Sri Lankan contexts. Initially, this chapter covers the research background, problem statement, research objectives, and research contribution. Then a high-level structure of the whole research report is depicted each chapter-wise. It enables readers to understand the flow of this report easily. Finally, the chapter conclusion is provided at the end of the chapter.

1.1 Background

One of the significant reasons for using the internet is for communication purposes. Social media communication plays a large role in internet usage (Bosse, Renner, & Wilkens, 2020). Social media sites consist of social network sites, media sharing platforms, blogs or weblogs, micro-blogging, wiki technologies, virtual worlds, location-based services, social bookmarking services, group buying/collective buying platforms, writing communities platforms, review sites, and the internet forum/message (Paliszkiewicz, & Koohang, 2016; as cited by Koohang, Paliszkiewicz, & Goluchowski, 2018). The total social media user projection for the year 2021 is 3.78 billion (Tankovska, 2021, January 28) and 2.74 billion has been already using Facebook worldwide as of January 2021 making it the most popular social media platform nowadays (Kemp, 2021, January 27). Facebook is an initiative by Mark Zuckerberg that was released in 2004 providing limited access only to Harvard university students by then. Since it has evolved immensely and now become the most popular social media platform in the world (Jim Wu et al., 2015; as cited by Chen, Tsai, & Chen, 2016). Social media sites like Facebook have stored a large amount of personal data and thereby they have become the main target of hackers (Nyoni & Velempini, 2018). The Facebook platform allows users to control their profile and personal data via Facebook privacy settings. These settings allow users to control their information visibility level to others ranging from friends to total strangers (Lewis, Kaufman & Christakis 2008; as cited by Kimberley & Karl van der, 2020). But yet 87 million user data has reportedly been misused by Cambridge Analytica and 30 million user data was exposed to third parties due to a

vulnerability associated with the “view as” functionality of Facebook profile in 2018 (ENISA, 2018). Socialarks, a Chinese social media management company has victimized a data leakage of 81.5 million Facebook user profiles in 2021. That data leakage has exposed over 40 million phone numbers and 32 million email addresses. Furthermore, the exposed records consist of users’ full names, “About” text, Facebook link with profile pictures, located country, messenger ID, website link, profile descriptions, like, follow, and rating count as well (Wilson, 2021, January 11). 533 million Facebook user details belong to 106 nations have been leaked online. This leaked information includes their full names, locations, birth dates, bios, and email addresses (1News, 2021). These kinds of incidents notify that in-built security mechanisms in Facebook are not always sufficient for Facebook users to safeguard themselves from cyber threats. Also, majority of Facebook users are unaware of that their posts and updates are in the public domain and they can be accessed easily. Therefore it is critical to improve Facebook user awareness in privacy awareness to safeguard them from potential property loss or surveillance (Nyoni & Velempini, 2018). Generally, Facebook users concerns of their privacy in Facebook and treat it as less trustworthy. However, still that doesn’t impact their Facebook usage. Here the privacy loss is acceptable for them as users’ social interaction desires are more powerful than that (O’Brien and Torres, 2012; as cited by Presthus & Vatne, 2019). Hence, all Facebook users need to take necessary precautions to safeguard their data and privacy from users’ points of view as well. The most powerful user privacy protection strategy in social media platforms falls into users' own hands. Only they can control what they publish and to whom on those platforms (Pensa & Di Blasi, 2017). Therefore, it is better if all the users can follow a set of recommended practices when using Facebook to reduce the impact of possible cyber threats. Hence, it is ideal to research to identify current user behavior and awareness in Facebook, user vulnerabilities they face based on their current behavior, and recommend best practices for users to protect themselves from those vulnerabilities.

1.2 Problem Statement

As stated before, it is critical to improving Facebook user awareness in privacy to safeguard them from potential property loss or surveillance as the majority of Facebook users are unaware that their posts and updates are in the public domain and can be accessed easily (Nyoni & Velempini, 2018). Also, privacy loss is acceptable as users’ social interaction desires are more powerful than privacy loss when using Facebook (O’Brien and Torres, 2012; as cited by Presthus & Vatne, 2019). These citations confirm that all the users are vulnerable

to various cyber threats willingly or unwillingly when they use the Facebook platform. The Facebook creators have mentioned that privacy is not as important when it comes to the values that the site offers according to a past statement. Service personalization and target advertising on Facebook are mostly based on the personal information of the users (Johnson, 2016; as cited by Nyoni & Velempini, 2018). This citation confirms that the user data are at risk in the Facebook platform and they can be altered or used for anything harmful if they fall into wrong hands. Hence, proper and updated cyber awareness and behavior in the Facebook platform is convenient for its users to protect their privacy and personal data against various cyber threats presented in the platform. The main problem that arises here is whether there is any updated solution available to address how Facebook users can safeguard themselves by following a set of recommended practices. Comprehensive research is conducted by the researcher on existing literature to identify any presented solution for his problem. There the researcher found some previous research articles that recognized cybersecurity best practices for users when using the internet. Some of those articles are relevant to social media usage as well. However, no research article is found related to the recommended practices when using the Facebook platform from users' point of view as per the knowledge of the researcher and from the pool of previous articles reviewed related to this research topic. Therefore, this aspect needs further research and the problem statement is formed based on that justification.

1.3 Research Objectives

Three major objectives are achieved through this research project as follows.

- Identification of current awareness and practices of Facebook users related to their profile in terms of cybersecurity.
- Identification of the vulnerability level of Facebook users based on their current cyber behavior.
- Recommendation of cybersecurity practices to overcome the identified vulnerability level from the user's point of view.

1.4 Research Contribution

There is a research gap in identifying recommended practices when using the Facebook platform from the user's point of view. The primary intention of the researcher is to address the aforementioned research gap by conducting this research project. As a result, this research contributes new knowledge to the existing literature by filling the research gap through research results and findings.

1.5 High-level Structure of Overall Research Report

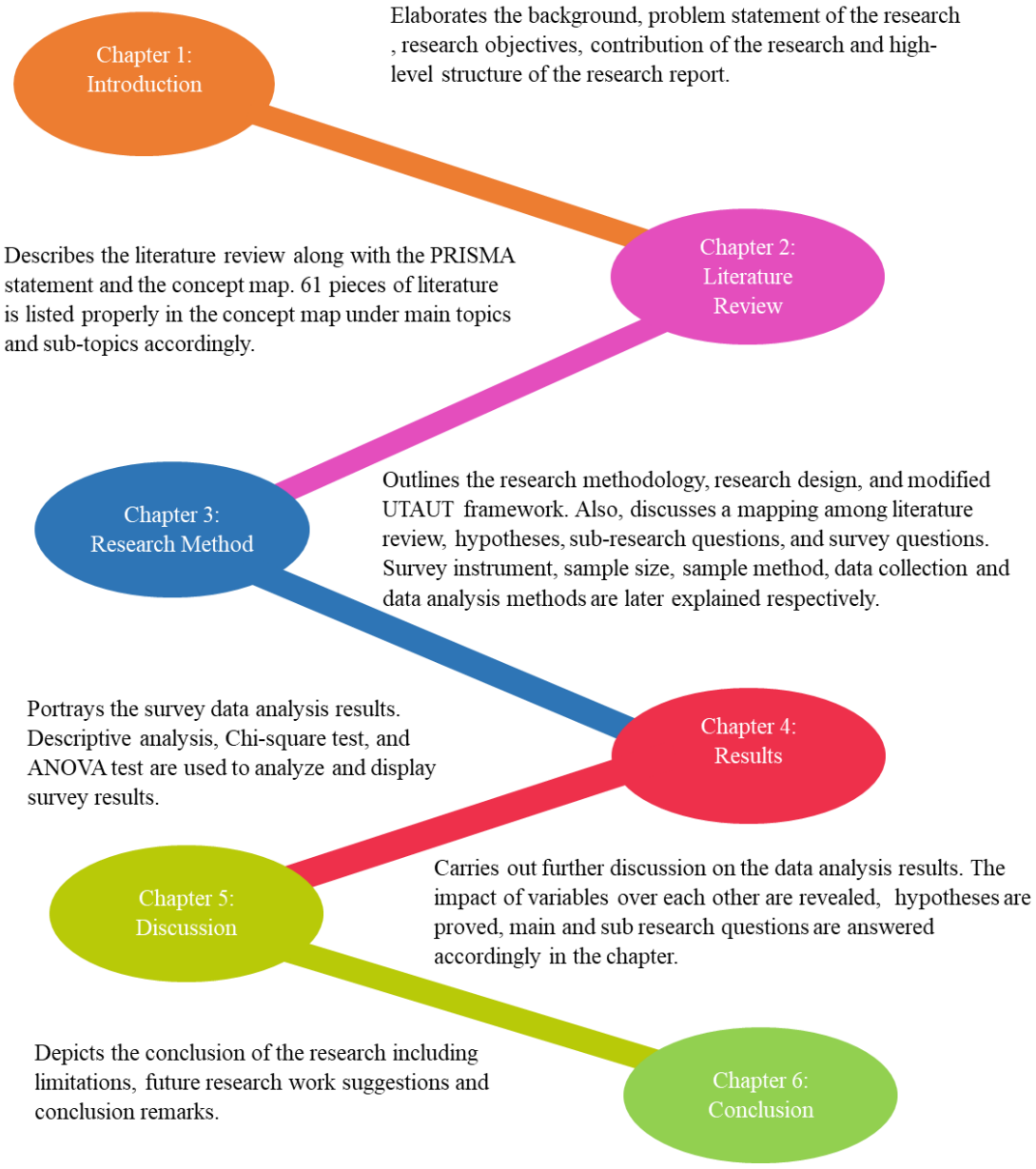


Figure 1.1: Outline of the research report

1.6 Conclusion

The number of cybercrimes in Facebook arises each day although it has an in-built security framework. Therefore, identifying a recommended set of practices when using Facebook from the user's point of view is critical. The next chapter covers literature reviews to support the research scope by identifying early research done mainly in the fields of cyber threats, cyber awareness, and cyber behavior regarding the internet, social media, and Facebook.

2. Literature Review

A systematic literature review is presented in this chapter in terms of PRISMA statement, concept map, themes, and sub-themes of concept map accordingly. Section 2.1 depicts how the articles are found based on the PRISMA statement along with inclusion and exclusion criteria. Section 2.2 portrays the themes and sub-themes of the literature review in terms of a concept map. Main subsection 2.2.1 illustrates the literature on common cyber threats on the internet. In subsection 2.2.1.1, it is explained the literature on cyber threats related to social media platforms. Next main subsection 2.2.2. discusses cybersecurity on the internet along with two other subsections where 2.2.2.1 outlines user awareness when using the internet and 2.2.2.2 describes the user behavior when using the internet respectively. The final main subsection 2.2.3 illustrates cybersecurity in social media. Then subsection 2.2.3.1 explains user awareness when using social media. Under that subsection 2.2.3.1.1 depicts the user awareness when using Facebook. Final subsection 2.2.3.2 portrays the user behavior when using social media while subsection 2.2.3.2.1 describes the user behavior when using Facebook. The main research question and sub-research questions are formed based on the literature found in the next 2.3 subsections. Final section 2.4 concludes the systematic literature review chapter.

2.1 PRISMA Statement

Systematic reviews ensure complete and transparent reporting of research (Rafael, Ferrán, Edoardo, & Craig, 2021). Searching literature is a significant component of a systematic review. The commonly used literature search component is the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) Statement (Melissa et al., 2021). PRISMA statement is a road map that supports authors explaining what was done, what was found, and what are they planning to do (Rafael et al., 2021). PRISMA checklist is a tool that can be used to guide the systematic review reporting and perform a meta-analysis on randomized controlled trials (Rice, Kloda, Shrier, & Thombs, 2016). As such, the PRIZMA statement supports this research when filtering appropriate and quality literature reviews systematically.

The main online databases used to find appropriate academic articles are Wintec OneSearch and google scholar. Also, some other reputed websites are referred to find up-to-date statistics relevant to the research. Keywords are used in the article search along with "AND" and "OR" operators to make the article search more relevant and precise. More than 10, 000 articles are found in the initial search from both databases, and only 2500

articles are filtered after removing duplicates. Wintec OneSearch database automatically removes duplicates from the search when the researcher moves forward with the search results. There the researcher found close to 2000 most relevant articles for the research report. Then the article search in Google Scholar is commenced and the researcher ignored the duplicated articles manually that are similar to the ones found in the Wintec OneSearch database. Then the researcher found around 500 most relevant articles for the research report from the Google Scholar database. From that pool, only 339 most relevant articles are screened and 130 articles are omitted due to the abstract ineligibility. Next, 209 relevant articles are filtered from the pool of screened articles, and 149 of them are disregarded due to the exclusion criteria as listed in Table 2.1. Finally, 61 articles are selected as the most eligible ones to include in the literature review representing all the main themes and sub-themes in the concept map.

Table 2.1: PRISMA statement's inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Peer-reviewed articles with full access rights	Articles asking for payments for the access
Published time in between 2015-2021	Published outside the intended time frame
Language: English	Other languages
Full-Text	Articles with no Full-text availability
Include relevant keywords	Not relevant to the literature themes
Original publication	Non-empirical studies

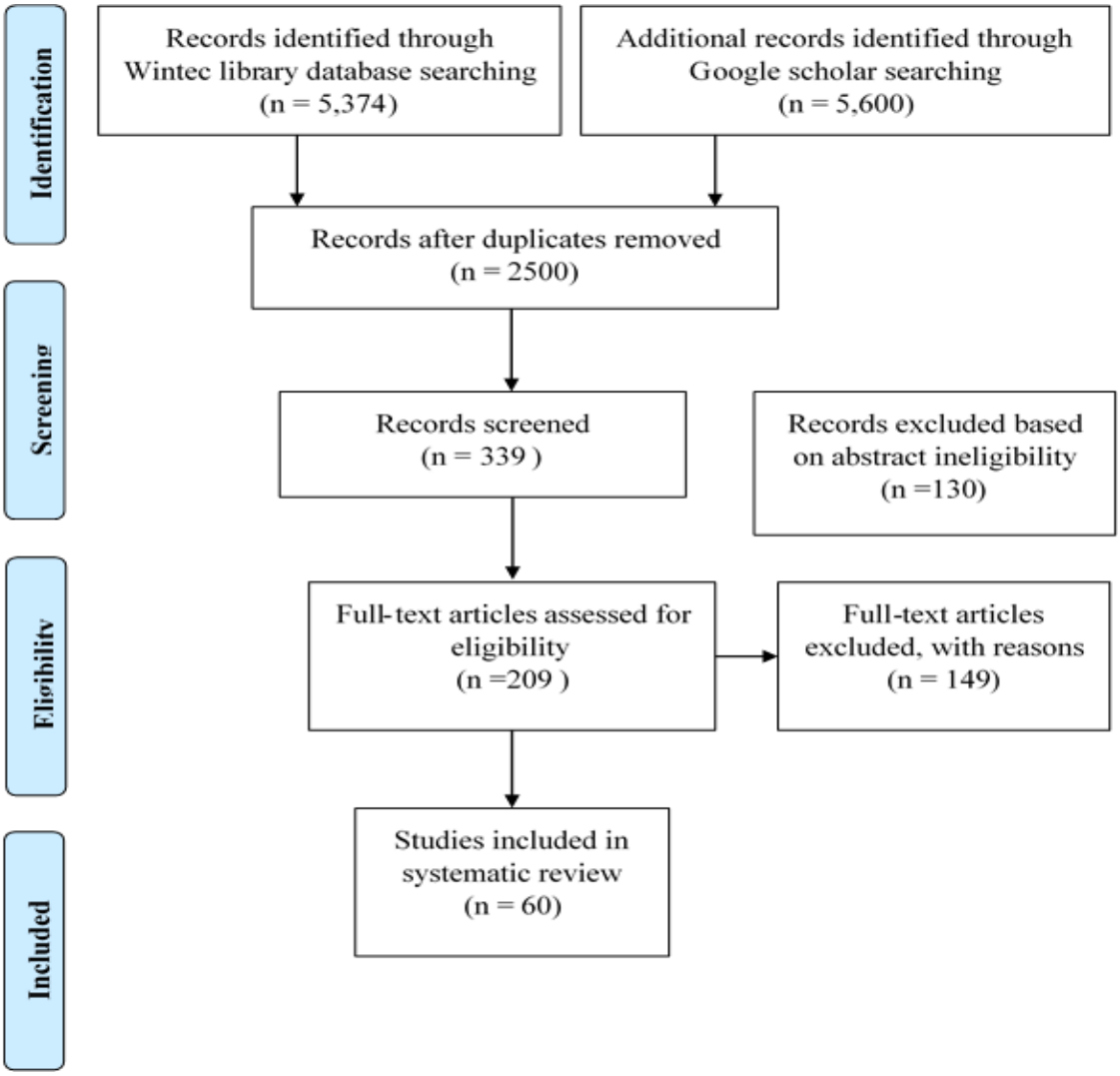


Figure 2.1: PRISMA flow chart

2.2 Literature Theme and Sub-theme

Literature found in the PRISMA statement is visualized in terms of a concept map in this section. Finalized literature is listed under relevant themes and sub-themes using a critical literature review analysis as per Figure 3. This makes the readers to refer each piece of literature easily as per their preference.

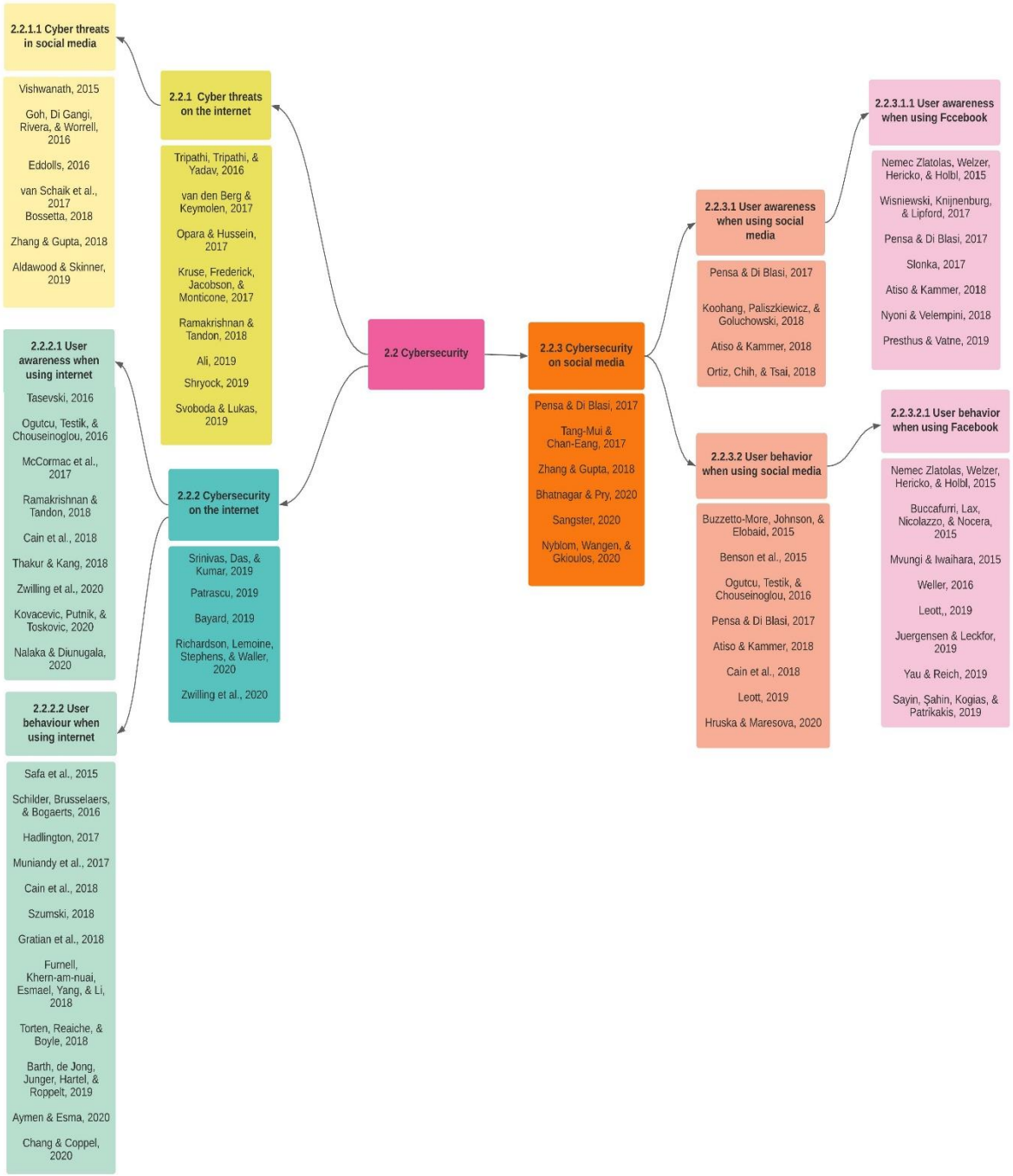


Figure 2.2: Concept map

All the pieces of literature listed in the concept map are elaborated in detail under each theme and sub-theme subsequently in this chapter.

2.2.1 Cyberthreats on the Internet

The first step of this research is to identify the presence of cyber threats in the world of the internet. Therefore, this subsection is designed to identify the origin of cybercrimes and commonly available cyber threats/cybercrimes within the internet via past works of literature.

Table 2.2.1 Theme article table: Cyberthreats on the internet

Author and year	Article name	Key findings	Research area	Research Method
Tripathi, Tripathi, & Yadav (2016)	Role of information technology in cyber crime and ethical issues in cyberethics	Types of cyber threats and the role of information technology act 2000 of India to discourage cyber threats	Cybercrimes and cyberethics	Qualitative
van den Berg & Keymolen, (2017)	Regulating security on the Internet: Control versus trust.	Trust is a key element in cybersecurity strategies	Cybersecurity	Qualitative
Opara & Hussein (2017)	Cybersecurity, threat intelligence: Defending the digital platform.	IT security professionals should be equipped with both security tools and up-to-date cybersecurity knowledge	Cybersecurity and threat intelligence	Quantitative
Kruse, Frederick, Jacobson, & Monticone (2017)	Cybersecurity in healthcare: A systematic review of modern threats and trends	The Healthcare industry should strengthen its cybersecurity practices regularly	Cybersecurity threats and trends in the healthcare industry	Qualitative
Ramakrishnan & Tandon (2018)	The evolving landscape of cyber threats	Major cyber threats available on the internet nowadays and the importance of cyber awareness	Cyber threats and user awareness	Qualitative

Ali (2019)	A constant threat for the business sector and its growth (A study of the online banking sector in GCC)	Need of high- level security framework for online banking in Gulf Cooperation Council (GCC)	Cybercrimes and cybersecurity in online banking	Quantitative
Shryock (2019)	The growing cyber threat: Practices are increasingly coming under attack by cybercriminals	Medical practices should take necessary precautions to protect against growing cyber threats as a part of a broad cybersecurity plan	Growing cyber threats	Qualitative
Svoboda & Lukas (2019)	Sources of threats and threats in cybersecurity.	Sources of cyber threats and types of cyber threats emerging from those sources	Cyber threats	Qualitative

Cybercrimes evolved with the development of the IT industry in the late 1970s. Initially, cyber crimes have emerged as spam, and then they have advanced up to viruses and malware now (Jobs, 2016; as cited by Kruse, Frederick, Jacobson, & Monticone, 2017). The word "Cyber Crimes" covers a vast range of virtual illegal activities performed by cybercriminals via any source of internet and electronic device (Ali, 2019). Hackers are using creative and different ways to collect personal data from gullible users (Ramakrishnan & Tandon, 2018). Experts say that cybercriminals have possessed many sources, high level of knowledge on how the technology works and its vulnerabilities. However, they tend to frame easy targets with the least resistance since it requires less effort to do the hacking (Shryock, 2019). The Internet has become an essential part of society and it has become the core of connecting and sharing information in modern days. This leads the internet to become a target of various cyber threats ranging from cybercrimes (hacking, identity theft, and other forms of fraud) to cyber-espionage, cyber-terrorism, and cyber-warfare (van den Berg & Keymolen, 2017). Cyber espionage has now become the "digital gold" for hackers and information breaches damage cyber victims' money and time in advance (Opara & Hussein, 2017). Cybercrimes

cover various cyber threats including child pornography, fraud, e-mails abuse, missing children, stalking, copyright, violation, harassment, threats, children abuse hacking, viruses, and many more (Tripathi, Tripathi, & Yadav, 2016). The impact of cyber threats is changing based on globalization, imposed security environment level, awareness, and the education level of administrators and users of the particular information and communication environment. These cyber-threats can range from privacy loss, personal, confidential, and classified data loss and fund/cryptocurrency loss to harm to the health and/or life of a person (Svoboda & Lukas, 2019).

2.2.1.1 Cyber Threats in Social Media

A huge number of cyber threats exist within social media nowadays. It is identified that most of the cyber threats on the Internet are relevant to social media platforms as well. This section mainly covers the social media risks and types of common cyber threats faced by social media users based on previous research findings.

Table 2.2.1.1 Theme article table: Cyberthreats in Social Media

Author and year	Article name	Key findings	Research area	Research Method
Vishwanath (2015)	Habitual Facebook use and its impact on getting deceived on social media	Interacting frequently with social media platforms, a high number of friends, and addiction to social media are the primary causes of habitual Facebook use. This behavior makes them vulnerable to level 1 and 2 social media phishing attacks.	Habitual Facebook use leading phishing attacks in Facebook	Quantitative
Goh, Di Gangi, Rivera, &	Graduate student perceptions of personal social	Risks inherited in social media	Cyber risks/threats in social media	Mixed

Worrell (2016)	media risk: A comparison study.			
Eddolls (2016)	Making cybercrime prevention the highest priority	Evolving cyber threats and defensive mechanisms to minimizing the impact	Cybercrimes and preventive measures	Qualitative
van Schaik et al. (2017)	Risk perceptions of cyber-security and precautionary behavior	Cyber awareness leads to precautionary cyber behavior and thereby protect users from cyber risks	Cybersecurity risks and relevant precautionary behaviors	Quantitative
Bossetta (2018)	The weaponization of social media: Spear phishing and cyber-attacks on democracy	How political forces can weaponize social media platforms to perform spear-phishing campaigns	Social media and spear phishing	Qualitative
Zhang & Gupta (2018)	Social media security and trustworthiness: Overview and new direction	Social media security and trustworthiness make users safe within the platform	Social media security	Quantitative
Aldawood & Skinner (2019)	Reviewing cybersecurity social engineering training and awareness programs—Pitfalls and ongoing issues	Staff accessing social media using company interconnected information systems can draw the attention of social engineers to commence attacks on those systems.	Social engineering attacks on social media	Qualitative

Social media risks can be identified with two major categories namely social risks and technology risks. Social risks further can be identified at an individual level such as loss of productivity, cyberbullying, cyberstalking, identity theft, social information overload, and at

a professional level such as inconsistent personal branding, personal reputational damage, data breach. Technology risks mainly include malicious software, service interruptions, hacks, and unauthorized access to social media accounts (van Zyl, 2009; Krasnova et al., 2009; Hogben,2007; Krasnova et al., 2009; Boyd, 2008; Argenti & Druckenbiller, 2004; Aula, 2010; Boyd, 2008; Hogben, 2007; Rivera et al., 2015; as cited by Goh, Di Gangi, Rivera, & Worrell, 2016). Most people reuse the same obscure password for all of their login activities including their employer's network. Cracking a password becomes easy with a hacker who possessed the right software tools and few personal data gained from one's social media (Eddolls, 2016). Fake accounts, cyberbullying, and sexual harassments are some of the major malicious behaviors that can be identified within the social media sphere (van Schaik et al., 2017). Various cyberattacks are presented in social media such as identity theft, spam attacks, malware attacks, Sybil attacks, social phishing, impersonation, hijacking, fake requests, and image retrieval and analysis (Zhang & Gupta, 2018). Social media users are exposed to so many cyber threats as for the aforementioned citations. Therefore an acceptable level of cyber awareness and cyber behavior is required when using those platforms. The presence of these threats confirms the requirement of identifying recommended practices in social media use. Social media has become a major playground for spear phishing attacks as it contains a large amount of public data. These data are used by imposters to create fake accounts to align with the personal and professional interests of the majority of social media users. Then they reach the target audience via various communication methods including friend requests, direct messaging, or target advertising. Users' reactions to these communications are critical since the attacker may deceive users to reveal their information or make them click malicious links (Bossetta, 2018). Phishing attackers can collect information related not only to the victimized user but also to other individuals who are connected with him/her due to the network nature of social media platforms (Vishwanath, 2015). Social engineering refers to a method of which taking advantage of weak and naïve human behavior. The correlation between social engineering and social media platforms such as Twitter, Snapchat, and Facebook has increased lately (Wilcox, Bhattacharya, & Islam, 2014; as cited byAldawood & Skinner, 2019). Mindful cyber awareness accompanied by secured cyber behavior is significantly required to be safe from this kind of situation. Otherwise, users are always in the high-risk zone in terms of the safety of social media.

2.2.2 Cybersecurity on the Internet

This section portrays cybersecurity on the internet as a whole. Mainly it covers the definition of cybersecurity, components in a cybersecurity environment, the importance of cybersecurity, and the significant impact of the human factor over cybersecurity.

Table 2.2.2 Theme article table: Cybersecurity on the Internet

Author and year	Article name	Key findings	Research area	Research Method
Srinivas, Das, & Kumar (2019)	Government regulations in cybersecurity: Framework, standards, and recommendations	Types of cyber-attacks, the role of cybersecurity incident management framework and elements of cybersecurity standard	Cybersecurity	Qualitative
Patrascu (2019)	Promoting cybersecurity culture through education	Formal, informal, and non-formal education can promote a cybersecurity culture for any user in any age	Cybersecurity	Qualitative
Bayard (2019)	The rise of cybercrime and the need for state cybersecurity regulations	Cyber threats, existing federal and state cybersecurity regulations, and the importance of imposing cybersecurity regulations to reduce the impact of cyber threats	Cyber threats and cybersecurity regulations	Qualitative
Richardson, Lemoine, Stephens, & Waller (2020)	Planning for cybersecurity in schools: The human factor.	The human factor should be given the same priority as same as technical	Cybersecurity and human factor	Qualitative

		advancements in schools when enhancing cybersecurity		
Zwilling et al. (2020)	Cybersecurity awareness, knowledge, and behavior: A Comparative Study	People with more cyber awareness and knowledge showed less vulnerable cyber behaviors	Cybersecurity awareness, knowledge, and behavior	Quantitative

Cybersecurity is a collection of techniques that have been established to protect the user or organizational cyber environment. (Seemma, Nandhini, & Sowmiya, 2018; as cited by Richardson, Lemoine, Stephens, & Waller, 2020). Cybersecurity protects not only information systems consist of hardware, software, and related infrastructure but also the data stored in such systems as well as the services provided by them from any illegal access, harm, or misuse (Deibert, & Rohozinski, 2010; as cited by Srinivas, Das, & Kumar, 2019). Having a cybersecurity culture covering information systems, computer networks, user data, and internet users is important since it will help to protect those categories effectively (Patrascu, 2019). Most people have an online life nowadays and they share most of their life events and details in it. Therefore, they can be misused by attackers easily if they are not well protected. Even though it says that there is no perfect defense against cyber-attacks most of them are preventable or at least better handled (Kenyon, 2018; as cited by Bayard, 2019). The impact of security breaches cannot be fully eliminated by just using security tools in computers and infrastructure. Because human error is the weakest link in the cybersecurity chain (Furnell et al., 2006; Parsons et al., 2014; Schultz, 2005; Anwar et al., 2017; Herath, & Rao, 2009; Schneie, 2004; as cited by Zwilling et al., 2020). This emphasizes the important role that should be performed by users to ensure cybersecurity in all internet activities.

2.2.2.1 User Awareness When Using the Internet

The importance of cyber awareness and factors affecting cyber awareness is covered in this subsection based on some previous works of literature. Also, three sub Research Questions (RQ)s namely RQ 1.1, RQ 1.2, and RQ 1.3 are identified and formed backed by the relevant literature in this subsection accordingly.

Table 2.2.2.1 Theme article table: User Awareness When Using the Internet

Author and year	Article name	Key findings	Research area	Research Method
Tasevski (2016)	IT and cyber security awareness-raising campaigns	Cybersecurity situational awareness is a significant factor in cyber awareness.	Cyber awareness	Qualitative
Ogutcu, Testik, & Chouseinoglou (2016)	Analysis of personal information security behavior and awareness	Higher education level higher the information security awareness	Information security awareness and behavior	Quantitative
McCormac et al. (2017)	Individual differences and information security awareness.	Information security awareness differs with individual differences including age, gender, personality, and risk-taking propensity	Information security awareness	Quantitative
Ramakrishnan & Tandon (2018)	The evolving landscape of cyber threats	Major cyber threats available on the internet nowadays and the importance of cyber awareness	Cyber threats and user awareness	Qualitative
Cain et al. (2018)	An exploratory study of cyber hygiene behaviors and knowledge	Cyber hygiene behaviors and knowledge differs based on age, gender, experience in cyber-attacks, and self-described expert level	Cyber hygiene behaviors and knowledge	Quantitative

Thakur & Kang (2018)	Gender and locale differences in cybercrime awareness among adolescents	Girls had a higher level of cyber awareness while boys had a medium level of cyber awareness	Cyber awareness	Quantitative
Kovacevic, Putnik, & Toskovic (2020)	Factors related to cyber security behavior	The participants of the survey knew that their data is not safe but still that did not alarm them to learn more about cybersecurity	Cyber awareness and cyber behavior	Quantitative
Nalaka & Diunugala (2020)	Factors associating with social media related crime victimization: Evidence from the undergraduates at a public university in Sri Lanka	The probability of becoming a cyber-victim of the youth is more than 50% and online security awareness among the youth generation is less	Cyber victimization	Quantitative

Cybersecurity awareness is the level of understanding achieved by users regarding the significance of information security, their associated responsibilities, and series of acts to practice an adequate degree of information security control to safeguard organizational data and networks (Shaw et al., 2009; as cited by Zwilling et al., 2020). Awareness is the first level of defense supporting the security of information systems and networks. Cybersecurity situational awareness on the internet is significant as it helps to prevent the compromise of data, information, knowledge, and wisdom (Tasevski, 2016). The older adults had higher Information Security Awareness (ISA) scores than young adults. A small significant difference was found in the ISA score related to gender where females claim more ISA score compared to males (McCormac et al., 2017). In contrast to this citation, another research article stated otherwise. Males have more cyber hygiene knowledge than females. However, surprisingly there was no difference in cyber hygiene knowledge among different age groups

(Cain, Edwards, & Still, 2018). In the research, it is found that higher education levels lead to higher information security awareness of the users. It is revealed that education level or information security training reduces risky user behavior (Ogutcu, Testik, & Chouseinoglou, 2016). In the multinomial regression analysis, it is found that people with more higher education and who are not living in their own-occupied housing are more often fallen into to cybercrime victims category (Oksanen, & Keipi, 2013, as cited by Nalaka & Diunugala, 2020). Internet users are always required to be updated with cyber threats as new threats are emerging and existing threats are evolving frequently. Unfortunately, most users have failed to achieve an acceptable level of protection comparing to the increasing rate of threats (Ramakrishnan & Tandon, 2018). Human beings are the central figure of cybersecurity and they should be highly equipped with security awareness to mitigate the risks they face in cyberspace (Kovacevic, Putnik, & Toskovic, 2020). Lack of awareness of cyber risks, usage of third-party apps, information distributed in social media, and web pages direct hackers to easily exploit these vulnerable users (Shaw et al., 2009; as cited by Zwilling et al., 2020). Lack of awareness in cybercrimes can lead to high-level damage to finances, emotions, ethical or moral values of users (Thakur & Kang, 2018).

2.2.2.2 User Behavior When Using the Internet

This subsection outlines the common user behavior when using the internet and the impact of cyber awareness over cyber behavior based on previous literature. Further, this subsection is supported to form sub RQ 1.4 backed by related literature accordingly.

Table 2.2.2.2 Theme article table: User Behavior When Using the Internet

Author and year	Article name	Key findings	Research area	Research Method
Safa et al. (2015)	Information security-conscious care behavior formation in organizations	Awareness plays a significant role in information security behavior	Information security behavior	Mixed
Schilder, Brusselaers, & Bogaerts (2016)	The effectiveness of an intervention to promote awareness and	Awareness was connected with a lower number of	Online awareness and behavior	Quantitative

	reduce online risk behavior in early adolescence	reported online risk behavior		
Hadlington (2017)	Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors	Internet addiction leads to a risky cybersecurity behavior	Human factors leading to risky cybersecurity behaviors	Quantitative
Muniandy et al. (2017)	Cybersecurity behavior among higher education students in Malaysia	Some vulnerable cyber behaviors can be reduced by proper cyber awareness	Cybersecurity behavior	Quantitative
Cain et al. (2018)	An exploratory study of cyber hygiene behaviors and knowledge	Cyber hygiene behaviors and knowledge differs based on age, gender, experience in cyber-attacks, and self-described expert level	Cyber hygiene behaviors and knowledge	Quantitative
Szumski (2018)	Cybersecurity best practices among Polish students	Most of the cybersecurity-related information flows from unreliable resources	Cybersecurity best practices	Quantitative
Gratian et al. (2018)	Correlating human traits and	Rational	Cybersecurity behavior	Quantitative

	cybersecurity behavior intentions.	decision-making and gender were major predictors of good security behavior intentions, while ethical risk-taking was often not a major predictor		
Furnell, Khern-am-nuai, Esmael, Yang, & Li (2018)	Enhancing security behavior by supporting the user	Users expected use of security features can be enhanced by proper guidance, feedback, explaining their security options and decisions	Security behavior	Quantitative
Torten, Reaiche, & Boyle (2018)	The impact of security awareness on information technology professionals' behavior	Countermeasure awareness should be the primary focus of security compliance training	Security awareness and behavior	Quantitative
Barth, de Jong, Junger, Hartel, & Roppelt (2019)	Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources	Users claim to be concerned about their data misuse but yet they are unwilling to invest their time and effort or money to protect their privacy	Online privacy and security behaviors	Quantitative
Aymen & Esma (2020)	Handling user-oriented cyber-attacks: STRIM, a	STRIM model helps to fulfill cybersecurity requirements by	User-based security training	Qualitative

	user-based security training model.	improving user awareness of various new and emerging cyber threats. Thereby model helps an organization to build security-conscious behavior among its employees.	model - STRIM	
Chang & Coppel (2020)	Building cybersecurity awareness in a developing country: Lessons from Myanmar	Cyber maturity and the culture of a particular country are significant when designing cybersecurity awareness campaigns	Cybersecurity awareness	Qualitative

Online privacy researches are found that users are interested in privacy protection but their actual behavior says otherwise. This inconsistency between expressed privacy concerns and actual, contradictory behavior is known as the privacy paradox (Barth and De Jong, 2017; Joinson et al., 2010; Tsai et al., 2006; as cited byBarth, de Jong, Junger, Hartel, & Roppelt, 2019). Intentional or unintentional vulnerable user behavior is one of the major issues in the information security sphere (Safa et al., 2015). As a key factor, information security awareness discusses the security awareness programs that impact on minimizing one's risky information security behavior (Kruger, & Kearney, 2006; as cited by Safa et al., 2015). Research results show that higher awareness was connected with a lower number of reported online risk behavior (Schilder, Brusselaers, & Bogaerts, 2016). In the research, it is identified that the cybersecurity behavior of the respondents potentially makes them vulnerable to cyber threats. But some of the threats could have been reduced with a proper level of awareness (Muniandy, Muniandy, & Samsudin, 2017). Lack of understanding regarding appropriate cybersecurity actions can lead end users to inappropriate cyber behavior (Debatin et al., 2009; Goodhue, & Straub, 1991; Hu, Hart, & Cooke, 2006; Straub, & Welke, 1998; as cited by Cain et al., 2018). The research findings revealed that user awareness improvements lead to

better security behavior (Furnell, Khern-am-nuai, Esmael, Yang, & Li, 2018). Security awareness impacts user behavior when protecting against risks in information security (Herath, & Rao, 2009; Thomson, & Solms, 1998; Puhakainen, & Siponene, 2010; as cited by Torten, Reaiche, & Boyle, 2018). There are three steps involved when adapting secured behavior on the internet. They are security awareness, education, and training (Sasse et al., 2007; as cited by Aymen & Esma, 2020). On the other hand, a study conducted by the Global Cyber Security Capacity Centre at the University of Oxford assumed that campaigns on cybersecurity awareness were unsuccessful in changing behavior (Bada et al., 2015; as cited by Chang & Coppel, 2020). Addiction to the internet leads to risky cybersecurity behavior. It is the driving factor that rises above all and controls personal thoughts, feelings, and behavior patterns (Giffiths, 2010; as cited by Hadlington, 2017). Older users have more secure behavior than younger users (Cain et al., 2018). Women and the age group between 18- 25 were more likely to show poorer security practices comparing to other demographic groups in the research (Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018). This becomes a critical factor when identifying what type of user is more vulnerable to cyber threats when conducting the research. 63% of the Polish students who have responded to the research mentioned that they use a “best practices" approach although this term is not clear and can be highly subjective. Because their main sources of cybersecurity knowledge come from either the internet, friends, or colleagues (Szumski, 2018). This citation is given the impression that there is less reliable resources for internet users to refer to get the proper and up-to-date knowledge on secure interet browsing. That makes the internet users more vulnerable to cyber threats with false believed secured cyber behavior lead by inaccurate sources of information.

2.2.3 Cybersecurity on Social Media

Definition of social media, users’ main aims of using the social media platforms, and the importance of cybersecurity in those platforms are covered in this subsection based on previous literature work found.

Table 2.2.3 Theme article table: Cybersecurity on Social Media

Author and year	Article name	Key findings	Research area	Research Method
Pensa & Di Blasi (2017)	A privacy self-assessment framework for online social networks	The most powerful privacy protectors in the social network platforms are the users themselves	User privacy in social networks	Quantitative
Tang-Mui & Chan-Eang (2017)	Impacts of social media (Facebook) on human communication and relationships: A view on behavioral change and social unity	Most respondents of the research were depending on Facebook in their daily life in terms of building relationships with friends and family, playing games, reading articles, accessing audio and video clips	Social media (Facebook) on human communication and relationships	Quantitative
Bhatnagar & Pry (2020)	Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study	Students are aware of the risks involved in social media. Also, they said that the security settings of social media are hard to understand and use.	Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media	Quantitative
Sangster (2020)	When it comes to cybersecurity, ignorance isn't bliss – it's negligence	Employees should be more careful with the data they share in social networks	Cybersecurity	Qualitative

Nyblom, Wangen, & Gkioulos (2020)	Risk perceptions on social media use in Norway	Reddit and Snapchat are the safest social media platforms while Facebook and Twitter are the riskiest in terms of risk perception	Risk perceptions on social media use	Quantitative

Social media is a collection of electronic communication platforms used by online users to create online communities. They use these platforms to share information, ideas, and personal messages with each other (Bhatnagar & Pry, 2020). The way of identifying the trade-off between protecting privacy and the use of social network potentials is yet to be achieved (Pensa & Di Blasi, 2017). Social media networks provide openness to user profiles and the data they share in the profile. However, this openness threatened user profiles being revealed and hacked (Tang-Mui & Chan-Eang, 2017). Most of the social media users are now addicted to sharing their ideas, sentiments, and experiments with a wide range of friends and friends of friends via videos and photos (Yan, 2016; as cited by Zhang & Gupta, 2018). This makes the need for cybersecurity more than ever in social media as most of their personal life is exposed to many unknown people in unknown destinations. People who post information online might not think of security risks associated with it primarily. But this action can voluntarily reveal more personal information to unknown people than they expected (Nyblom, Wangen, & Gkioulos, 2020). Employees should be more careful about what they share on social media since social engineering scams are rising gradually in modern days. Those data can be used against them and their company together with other personal data that the cybercriminals collected through other consumer data breaches (Wikipedia, 2020; as cited by Sangster, 2020).

2.2.3.1 User Awareness When Using Social Media

Having an appropriate level of user awareness when using social media is important. The level of user awareness in social media is revealed according to past works of literature in this subsection.

Table 2.2.3.1 Theme article table: User Awareness When Using Social Media

Author and year	Article name	Key findings	Research area	Research Method
Pensa & Di Blasi (2017)	A privacy self-assessment framework for online social networks	The most powerful privacy protectors in the social network platforms are the users themselves	User privacy in social networks	Quantitative
Koohang, Paliszkiewicz, & Goluchowski (2018)	Social media privacy concerns: trusting beliefs and risk beliefs	The secondary usage, improper access, awareness have a negative significant association with user's trusting beliefs while collection, errors, and improper access have a significant positive association with user's risk beliefs	Social media privacy concerns	Quantitative
Atiso & Kammer (2018)	User beware: Determining vulnerability in social media platforms for users in Ghana	Most social media users are unaware of vulnerabilities in those platforms	User vulnerabilities in social media	Qualitative
Ortiz, Chih, & Tsai (2018)	Information privacy, consumer alienation, and lurking behavior in social networking sites	Higher information security awareness leads social network users to protect themselves using threat appraisal and generating strong privacy risk belief	Information security awareness and behavior	Quantitative

Disclosing data that have been perceived as less sensitive in social media platforms by the users can also lead to privacy breaches and user awareness around that sphere is still insufficient. One common example for the above matter is GPS tagging of a place that a user is currently visiting may alarm thieves to commence a robbery in that user's home or apartment. Another example is disclosing family relationships in social media may lead to privacy issues like stalking, slander, and cyberbullying for that family member(s) (Pensa & Di Blasi, 2017). A stronger information security concern level can be achieved by a high level of privacy awareness (Boyd, & Hargittai, 2010; as cited by Ortiz, Chih, & Tsai, 2018). Disclosing personal information is often required to get the intended services from social media. This action involves risks related to possible user privacy breaches in those platforms (Joinson, 2008; as cited by Koohang et al., 2018). Most social media users are unaware of the risks and vulnerabilities associated with those platforms unless they have experienced those in their real lives (Atiso & Kammer, 2018).

2.2.3.1.1 User Awareness When Using Facebook

The core objective of this subsection is to identify the user awareness level of Facebook users according to past literature. As suggested by the literature it is discovered that most Facebook users have a lower level of user awareness. Their lack of awareness leads them not to take necessary protective measures when sharing personal information and to set up the appropriate level of privacy settings related to their Facebook profiles.

Table 2.2.3.1.1 Theme article table: User Awareness When Using Facebook

Author and year	Article name	Key findings	Research area	Research Method
Nemec Zlatolas, Welzer, Hericko, & Holbl (2015)	Privacy antecedents for SNS self-disclosure: The case of Facebook	Significant privacy variables causing self-disclosure in Facebook	Privacy variables causing self-disclosure in Facebook	Quantitative
Wisniewski, Knijnenburg, & Lipford (2017)	Making privacy personal: Profiling social network users to	Feature awareness was shown to be a significant predictor of corresponding	User awareness and user behavior	Quantitative

	information privacy education and nudging	privacy behaviors in Facebook		
Slonka (2017)	Awareness of malicious social engineering among Facebook users	Baby Boomers are highly unaware of malicious social engineering in Facebook than other younger generations	User awareness on malicious social engineering among Facebook users	Quantitative
Nyoni & Velempini (2018)	Privacy and user awareness on Facebook	Most of the users' data can be easily collected through Facebook since they are publicly available	Privacy and user awareness on Facebook	Mixed
Presthus & Vatne (2019)	A survey on Facebook users and information privacy	Disclosing personal data is mainly based on the user's awareness level	Information privacy of Facebook users	Quantitative

Sometimes Facebook users are unaware of the audience of their publishing posts (Johnson, Egelman, & Bellovin, 2012; as cited by Nemec Zlatolas, Welzer, Hericko, & Holbl, 2015). In the research, it is found that feature awareness is shown to be a significant predictor of corresponding privacy behaviors in Facebook (Wisniewski, Knijnenburg, & Lipford, 2017). Facebook former CTO Bret Taylor revealed that 13 million Facebook users had never set or did not aware of Facebook privacy tools in the USA in 2012. In another research, it has also found that 36% of Facebook content has been shared with default privacy settings and thereby exposed to more users than expected (Pensa & Di Blasi, 2017). People who have born between 1946-1962 are called "Baby Boomers" while people who are born between 1963-1978 are called "Generation X". People born between 1979-1992 are called "Generation Y" and people born after 1992 are called "Millennials".In the research, it is revealed that Baby Boomers are highly aware of malicious social engineering in Facebook

than other younger generations (Jorgensen, 2003; Paula, & Dominic 1999; Tucker, 2006; as cited by Slonka, 2017). On Facebook, users can file a complaint against a post or any person related to any unacceptable attitude or behavior. Users can also use the in-built features of the Facebook platform to hide such posts, block or unfriend such people from their accounts. Unfortunately, most of the users are unaware of such protective actions (Atiso & Kammer, 2018). Social media sites like Facebook have stored a large amount of personal data and thereby they have become the main target of hackers. These stolen data will be then sold to online marketers for financial gains (Nyoni & Velempini, 2018). Therefore users should be well aware of which data they share with what people on Facebook. Otherwise, they will become victims of cybercrimes before they get any clue. Disclosing personal data when using Facebook is a trade-off based on user awareness (Presthus & Vatne, 2019). There they further mention that it is a privacy trade-off and this fact makes user awareness is one of the major factors for safeguarding their privacy when using the platform.

2.2.3.2 User Behavior When Using Social Media

This subsection illustrates the literature based on user behavior when using social media. Also, this subsection establishes a ground to form RQ 1.5 backed by the listed literature.

Table 2.2.3.2 Theme article table: User Behavior When Using Social Media

Author and year	Article name	Key findings	Research area	Research Method
Buzzetto-More, Johnson, & Elobaid (2015)	Communicating and sharing in the semantic web: an examination of social media risks, consequences, and attitudinal awareness	College students practice several risky behaviors in social media	Social media risks, consequences, and attitudinal awareness	Quantitative
Benson et al. (2015)	Information disclosure of social media users	There is a negative relationship between the level of control over personal data and self-disclosure	Information disclosure of social media users	Quantitative

Leott (2019)	Screening out: Criminal justice students' awareness of social media usage in policing	Main purposes of Criminal justice students' social media usage	Social media usage	Quantitative
Hruska & Maresova (2020)	Use of Social Media Platforms among Adults in the United States—Behavior on Social Media	Social media usage decreases with age and the usage increases when income and education level increases	The behavior of social media users	Qualitative

Awareness of controlling privacy settings in social media is usually limited to the users and thereby limited in actual use as well (Pensa & Di Blasi, 2017). Unsafe activities of teens and young adults in social media may lead to privacy invasion, unauthorized disclosure of personal information, inappropriate self-disclosure, internet addiction, cyberbullying, stalking, scams, identity thefts, and defamation (Buzzetto-More, 20212; as cited by Buzzetto-More, Johnson, & Elobaid, 2015). High-level use of social network sites leads to a high level of self-disclosure (Trepte, & Reinecke, 2013; as cited by Benson, Saridakis, & Tennakoon, 2015). High-level usage of social media makes some users more vulnerable. Those vulnerabilities made them face scams and behave online in a fearful and distrusting manner (Kaplan, & Haenlein, 2010; as cited by Atiso & Kammer, 2018). Attackers always look for vulnerabilities like users with poor best practices or more self-disclosure. Most of the old and youth participants of the survey have revealed that they have shared too many personal details on social media including their phone numbers and addresses. The risky side of this behavior is that most of them do not check their privacy settings related to their social media accounts (Cain et al., 2018). So these kinds of behaviors lead them to become easy targets of cybercriminals if any data breach happens within those social media sites. Most of the undergraduates use social media platforms to connect with family and friends, initiate and sustain relationships, pass time, gain entertainment and express themselves (Park, & Lee, 2014; Sherrel,l & Lambie, 2016; Kushin, & Yamamoto, 2010; as cited by Leott, 2019). In the

research, it is found that the high-risk category includes students from age 18-30. A possible reason for this is the high usage of the internet especially social media and social networks (Ogutcu et al., 2016). Social media usage decreases with age and the usage increases when income and education level increase (Hruska & Maresova, 2020). This helps to identify the most vulnerable age groups and education levels when conducting the research.

2.2.3.2.1 User Behavior When Using Facebook

The past literature on user behavior particularly related to Facebook is discovered in this subsection. It is revealed that there are many risky user behaviors in Facebook which ultimately make users vulnerable to various cyber threats.

Table 2.2.3.2.1 Theme article table: User Behavior When Using Facebook

Author and year	Article name	Key findings	Research area	Research Method
Buccafurri, Lax, Nicolazzo, & Nocera (2015)	Comparing Twitter and Facebook user behavior: Privacy and other aspects	More user awareness leads to less self-disclosure	Twitter and Facebook user behavior	Quantitative
Mvungi & Iwaihara (2015)	Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features	younger aged people disclose more contact information in their profile to achieve more openness in Facebook platform	User awareness and behavior in Facebook	Quantitative
Weller (2016)	Trying to understand social media users and usage	Main motivations of using Facebook	Social media users and usage	Qualitative

Juergensen & Leckfor (2019)	Stop pushing me away: Relative level of Facebook addiction is associated with implicit approach motivation for Facebook stimuli	User behavior in social media	User behavior in social media	Quantitative
Yau & Reich (2019)	"It's just a lot of work": Adolescents' self-presentation norms and practices on Facebook and Instagram	Teens are more likely to present themselves as much as positive in social media	Self-presentation norms and practices in Facebook and Instagram	Quantitative
Sayin, Şahin, Kogias, & Patrikakis (2019)	Privacy issues in post dissemination on Facebook.	In Facebook personal information can be visible to people other than expected and personal interactions may be inaccessible to users.	Privacy issues in post dissemination on Facebook	Quantitative

There are two major motivations for using Facebook namely the need to belong and the need for self-presentation. (Hofmann, 2012; as cited by Weller, 2016). Facebook has become the most popular social media platform among adults. 72% of undergraduate college students use Facebook and among them, 70% visit the platform daily and 43% of them use it more than once a day (Duggan 2015; as cited by Leott, 2019) The social networking sites can lead to a user behavior where they commit more time on the site rather than studies/job, interpersonal relationships, and/or psychological health and well-being (Pallesen, 2014; as cited by Juergensen & Leckfor, 2019). This is realistic when it comes to Facebook as well. In the research, it is revealed that Facebook users put high trust in the Facebook platform itself and other Facebook users. Thus they tend to share identifying information confidently on the

platform (Dwyer et al., 2007; as cited by Buccafurri, Lax, Nicolazzo, & Nocera, 2015). Exposing contact information like mobile phone number, email and non-contact information like a birthday to unknown people in Facebook are considered as risky behavior. In the research, it is discovered that younger aged people disclose more contact information in their profiles to achieve more openness in the platform (Mvungi & Iwaihara, 2015). Many students allowed access to their addressed or personal pictures to random people on Facebook by not restricting access to their profiles accordingly (Acquisti, & Gross, 2006; Gross, & Acquisti, 2005; Kolek, & Saunders, 2008; as cited by Nemec Zlatolas et al., 2015). This behavior can be further analyzed and identify if there is any relationship between this behavior and becoming vulnerable to cyber threats on the Facebook platform. The Facebook privacy policy and Facebook users believe that all friends are reliable and predefined privacy settings remain the same. But if users do not properly configure their privacy settings in their user account accordingly, their posts can be seen by people even outside their social cycle. This action makes users vulnerable to privacy risks (Sayin, Şahin, Kogias, & Patrikakis, 2019). Teenagers are more often try to make a positive online image to gain more peer acceptance in social media like on Facebook. Also, the users' behavior in social media is mainly based on what they perceive to be true (Yau & Reich, 2019). For this reason, many young people can be easy targets of cybercriminals on social media platforms and this factor is further analyzed in this research.

2.3 Research questions

The above works of literature provide a base to develop below main RQ and sub RQs accordingly.

RQ1: What are the recommended cybersecurity practices for Facebook users from the user's point of view in the New Zealand and Sri Lankan contexts?

RQ 1.1: What is the impact of the user's age on cyber awareness when using Facebook?

RQ 1.2: What is the impact of the user's gender on cyber awareness when using Facebook?

RQ 1.3: What is the impact of the user's education level on cyber awareness when using Facebook?

RQ 1.4: What is the impact of the user's cyber awareness on the user's cyber behavior when using Facebook?

RQ 1.5: What is the impact of the user's cyber behavior on the user's vulnerability level when using Facebook?

Forming of RQ1, RQ1.1, RQ1.2, RQ1.3, RQ1.4, and RQ1.5 are further clarified in subsection 3.1 Research Questions and Hypotheses in the next chapter.

2.4 Conclusion

After identifying the relevant literature to the research, the next step is to work on the research methodology and research design. Therefore, the next chapter is dedicated to discussing the research methodology along with the main research question, sub–research questions, theoretical model, and overall research design with data analysis methods respectively.

3. Research Method

This chapter majorly illustrates the research methodology and research design. Subsection 3.1 describes the main research question, sub-research questions identified in the literature review section along with the hypothesis. Subsection 3.2 illustrates the research design including the modified theoretical framework. 3.3 depicts the research instrument used to collect real data from the target sample. Next, subsection 3.4 depicts the sampling method while subsection 3.5 explains how the researcher identified the sample size using an authentic method. Then the data collection description is provided in subsection 3.6. Primary data description and data analysis methods are explained in subsection 3.7 and 3.8 respectively. Finally, subsection 3.10 concludes the overall chapter 3.

3.1 Research Questions and Hypotheses

This research is mainly focusing on identifying recommended cybersecurity practices for Facebook users from the user's point of view. The current awareness and practices of Facebook users and the associated vulnerability level should be identified before recommending appropriate cybersecurity practices. For that, this research is designed to follow the post-positivist research method along with quantitative research methodology when conducting the research.

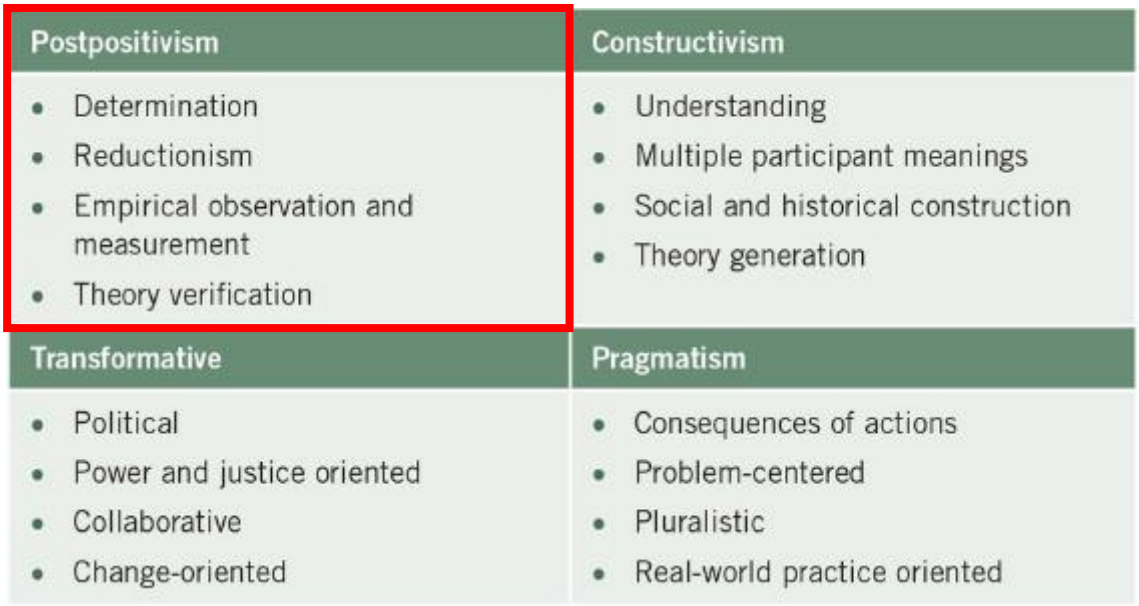


Figure 3.1: Four world views (Creswell & Creswell, 2018)

Post-positivist research is based on the belief that there is a single reality although it is doubtful (critical realist ontology) and pure objectivity is impossible (modified objectivist epistemology) (Sharma, 2010; as cited by Davies & Fisher, 2018). Post-positivist research recognizes human behavior is complex and unbiased, and objective reporting research was

not always possible (Clark, 1998; as cited by Davies & Fisher, 2018). Quantitative research methods concern structured data collection and analysis and they can be presented numerically (Goertzen, 2017). Quantitative research generates numeric data and tries to find correct answers through testing hypotheses using objective and impartial scientific methods (Davies & Fisher, 2018; as cited by Bloomfield & Fisher, 2019). Quantitative research is conducted within a more structured environment where researcher(s) are frequently allowed to control study variables, environment, and research questions (Polit & Beck, 2012; as cited by Rutberg & Bouikidis, 2018). This research is conducted to identify the impact of independent variables (age, gender, and education level), median variables (cyber awareness and cyber behavior), and a dependent variable (vulnerability level of the users) over each other using an already established theoretical framework. Also, a numeric presentation of survey data is significant to identify the impact of variables over each other via proving hypotheses. This also helps to answer relevant main and sub-RQs as well. Therefore, the post-positivist research method along with quantitative research methodology is the best way of conducting this research backed by the aforementioned citations.

The research topic of this report is the recommended cybersecurity practices for Facebook users from the user's point of view. There New Zealand and Sri Lanka were selected to research carefully considering three major reasons. The first one is due to the original geographical area of the research covers the whole world and the researcher wanted to narrow it down. The second reason is due to easy access to the survey participants in Sri Lanka and New Zealand based on the convenience sampling method and the final reason is due to the time limitation. There is no intention of comparing awareness, behavior, and vulnerability level between these countries based on age, gender, and education level. Hence, both countries are selected solely to collect data to identify Facebook user awareness, behavior, and vulnerability levels on a common basis.

The main RQ and sub-RQs are formed as below based on the facts found in the systematic literature review as in chapter 2.

RQ1: What are the recommended cybersecurity practices for Facebook users from the user's point of view in the New Zealand and Sri Lankan contexts?

Sub RQs are developed in a way to identify the impacts of independent variables over median variables and to identify the impact of median variables over respective dependent variables in the theoretical framework. This step is significant to identify variables to be focused on

when recommending practices for Facebook users to safeguard themselves from various cyber threats.

RQ 1.1: What is the impact of the user's age on cyber awareness when using Facebook?

RQ 1.2: What is the impact of the user's gender on cyber awareness when using Facebook?

RQ 1.3: What is the impact of the user's education level on cyber awareness when using Facebook?

RQ 1.4: What is the impact of the user's cyber awareness on the user's cyber behavior when using Facebook?

RQ 1.5: What is the impact of the user's cyber behavior on the user's vulnerability level when using Facebook?

Below mentions the hypotheses identified relevant to sub-RQs.

H1 – Age has no impact on the user's cyber awareness

H2 – Age has an impact on the user's cyber awareness

H3 – Gender has no impact on the user's cyber awareness

H4 – Gender has an impact on the user's cyber awareness

H5 – Education level has no impact on the user's cyber awareness

H6 – Education level has an impact on the user's cyber awareness

H7 - User's cyber awareness has no impact on the user's cyber behavior

H8- User's cyber awareness has an impact on the user's cyber behavior

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

A further explanation of forming hypotheses backed by literature is mentioned below.

The older adults had higher Information Security Awareness (ISA) scores than young adults. A small significant difference was found in the ISA score related to gender where females claim more ISA score compared to males (McCormac et al., 2017). In contrast to this citation, another research article stated otherwise. Males have more cyber hygiene knowledge than females. However, surprisingly there was no difference in cyber hygiene knowledge among different age groups (Cain, Edwards, & Still, 2018).

The above works of literature provide a base to develop H1, H2, H3, and H4 backed by the facts that age and gender may have an impact on cyber awareness or not.

H1 -Age has a positive impact on the user's cyber awareness

H2- Age has no impact on the user's cyber awareness

H3 – Gender has a positive impact on the user's cyber awareness

H4 - Gender has no impact on the user's cyber awareness

In the research, it is found that higher education levels lead to higher information security awareness of the users (Ogutcu, Testik, & Chouseinoglou, 2016). On the other hand, In the multinomial regression analysis, it is found that people with more higher education and who are not living in their own-occupied housing are more often fallen into to cybercrime victims category (Oksanen, & Keipi, 2013, as cited by Nalaka & Diunugala, 2020).

The above literature provides a base to develop H5, and H6 backed by the facts that education level may have an impact on cyber awareness or not.

H5 – Education level has a positive impact on the user's cyber awareness

H6 - Education level has no impact on the user's cyber awareness

Information security awareness is the key to minimize one's risky information security behavior (Safa et al., 2015). Research results show that higher awareness was connected with a lower number of reported online risk behavior (Schilder, Brusselaers, & Bogaerts, 2016). In the research, it is identified that the cybersecurity behavior of the respondents potentially makes them vulnerable to cyber threats. But some of the threats could have been reduced with a proper level of awareness (Muniandy, Muniandy, & Samsudin, 2017). Lack of awareness regarding appropriate cybersecurity actions can lead end users to inappropriate cyber behavior (Cain et al., 2018). The research findings revealed that user awareness improvements lead to better security behavior (Furnell, Khern-am-nuai, Esmael, Yang, & Li, 2018). Security awareness impacts user behavior when protecting against risks in information security based on the literature found (Torten, Reaiche, & Boyle, 2018). There are three steps involved when adapting secured behavior on the internet. They are security awareness, education, and training (Aymen & Esma, 2020). On the other hand, a study conducted by the Global Cyber Security Capacity Centre at the University of Oxford assumed that campaigns on cybersecurity awareness were unsuccessful in changing behavior (Chang & Coppel, 2020).

The above pieces of literature provide a base to develop H7 and H8 backed by the facts that user awareness has an impact on cyber behavior or not.

H7 – User's cyber awareness has a positive impact on the user's cyber behavior

H8 – User's cyber awareness has no impact on the user's cyber behavior

In the research, it is identified that the cybersecurity behavior of the respondents potentially makes them vulnerable to cyber threats (Muniandy et al., 2017). High-level usage of social media makes some users more vulnerable. Those vulnerabilities made them face scams and fearing and distrusting online behaviors (Atiso & Kammer, 2018). Attackers always look for vulnerabilities like users with poor best practices or more self-disclosure (Cain et al., 2018).

The above literature provides a base to develop H9 and H10 backed by the facts that user behavior has an impact on the user vulnerability level or not.

H9 – User's cyber behavior has a positive impact on the vulnerability level of the user on the Facebook platform

H10 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform User's cyber awareness has no impact on the user's cyber behavior

3.2 Research Design

A modified theoretical framework is developed based on the Unified Theory of Acceptance and Use of Technology model (UTAUT) when designing the research. UTAUT model has been accepted especially for technology acceptance testing (Venkatesh et al., 2003; as cited by Richa, 2020). Some elements of eight previous behavioral intention models related to technology acceptance are used when developing the UTAUT model. They are the Technology Acceptance Model (TAM), the Theory of Reasoned Action (TRA), the motivational model, the Theory of Planned Behavior (TPB), the model of Personal Computer (PC) utilization, innovation diffusion theory, the combined TAM, and TPB model, and models reflecting social cognition theory. There are six main constructs in the UTAUT model namely performance expectancy, effort expectancy, social influence, facilitating conditions, behavioral intention to use the system, and usage behavior (Oshlyansky et al., 2007; Venkatesh et al., 2003; as cited by Khalilzadeh, Ozturk, & Bilgihan, 2017). Behavioral and social factors are significant when understanding Social Network Sites (SNS). The UTAUT model captures the details of these control factors. Therefore UTAUT is the best theoretical framework for our study aimed at SNS adoption in different sociocultural settings (Kaba & Toure, 2014). The research mainly finds out that UTAUT is an effective theoretical model to understand users' willingness to accept Facebook in a Middle Eastern country (Al-Azawei,

2018). Therefore, the researcher also used a modified UTAUT framework mainly considering the social influence and usage behavior constructs to understand the current cyber awareness and cyber behavior of Facebook users and thereby identify their vulnerability level as depicted in Figure 3.2.

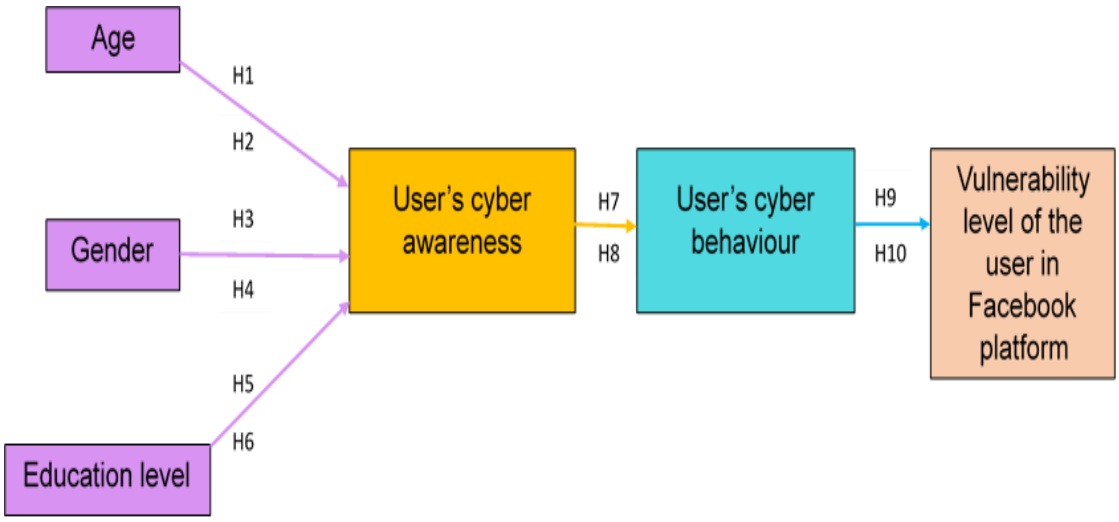


Figure 3.2: Modified UTAUT Model

The connection between variables, literature review (LR), hypotheses (H), and research questions (RQ) is further expanded and illustrated in Figure 5.

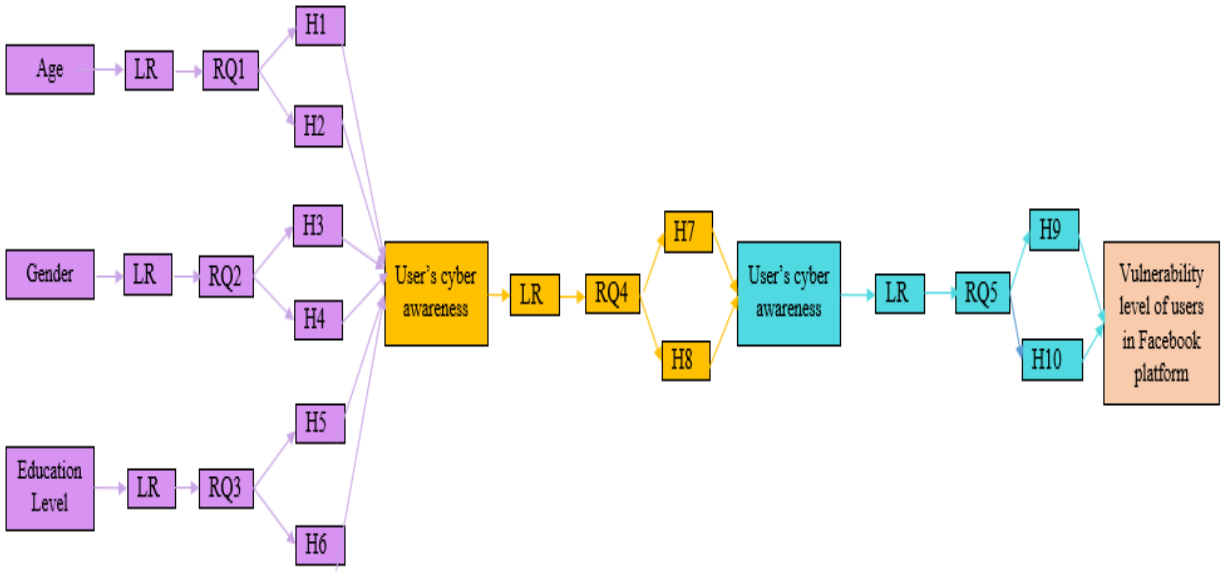


Figure 3.3: Connection between variables, LR, H, and RQ in the modified UTAUT model

The connection between the main RQ, literature review, H, sub-RQs, and survey questions is illustrated in a tabular format in Table 3.1.

Table 3.1 Connection between Main RQ, Literature review, Hypotheses, Sub-research questions, and survey questions

	Literature review	Hypotheses	Sub-research Questions	Survey question
Main research question	2.2.2.1	H1,H2	RQ 1.1	S1,S5,S7,S9,S11,S19
		H3,H4	RQ 1.2	S2, S5,S7,S9,S11,S19
		H5, H6	RQ 1.3	S3, S5,S7,S9,S11,S19
	2.2.2.2	H7, H8	RQ 1.4	S5,S6,S7,S8,S9,S10,S11,S12, S19, S20
	2.2.3.2	H9, H10	RQ 1.5	S22, S4, S6,S8,S10,S12,S13,S14,S15, S16, S17, S18, S20

3.3 Research Instrument

The research instrument used in this research is SSS. It consists of 3 screening questions, 21 closed-ended questions, and 1 semi-open-ended question. The first 3 questions of the survey are related to Facebook users' socio-demographic information including age, gender, and education level. The rest of the 19 questions are related to the current cyber awareness and cyber behavior of Facebook users in both New Zealand and Sri Lanka. Please refer the Appendix A for detailed SSS questions.

3.4 Sample Size

The Facebook population of New Zealand and Sri Lanka were considered when calculating sample size. As stated before this is due to narrow the scope of the research, time limitation, and easy access to the sample size. Total Facebook users above 18 years in New Zealand in March 2021 was 3 510 000. Facebook users in Sri Lanka over age 18 in March 2021 was 7 680 000. The source of data represented in this website is directly from the marketing APIs of the respective social platform (NapoleonCat, 2021). Table 3.2 illustrates the Facebook user distribution in New Zealand according to age and gender.

Table 3.2 New Zealand's age and gender wise Facebook user distribution (Source: NapoleonCat, 2021)

Age / Gender	18-24	25-34	35-44	45-54	55-64	65+
Female	350,000	450,000	330,000	290,000	240,000	220,000
Male	320,000	460,000	300,000	240,000	170,000	140,000

Table 3.3 illustrates the Facebook user distribution in Sri Lanka according to age and gender.

Table 3.3 Sri Lanka's age and gender wise Facebook user distribution (Source: NapoleonCat, 2021)

Age / Gender	18-24	25-34	35-44	45-54	55-64	65+
Female	720,000	970,000	550,000	230,000	110,000	55,000
Male	1,300,000	1,600,000	1,000,000	420,000	170,000	95,000

Hence, the sample size is calculated based on the 11.19 (3.51+7.68) million total Facebook user population in both countries and considering the confidence interval of 4 along with a confidence level of 95%. The resulted sample size was 600 as calculated by the sample calculator published by https://surveysystem.com/. However Covid-19 cases during the past nine weeks reach high and Sri Lanka is one of the new Covid-19 hotspots that emerged during the time (NZHerld, 2021, May 3). There is another news mentioned in the World Health Organization (WHO)'s site related to Sri Lanka's recent Covid-19 outbreak reported by Ms. Sahani Chandraratna, Health promotion, and communications officer, WHO country office. A trend of the rapid exponential increase of Covid-19 cases was noticed in Sri Lanka within the past few weeks. Health experts expect those figures will further increase in the coming weeks (Chandraratna, 2021, May 10). The number of new Covid-19 cases in Sri Lanka has been breaking records almost every day since April 17 (Mallapaty, 2021). As evidenced in the aforementioned citations, due to the recent Covid-19 outbreak in Sri Lanka and time limitation only 464 valid responses are collected through the online survey. As a result confidence interval is increased from 4 to 4.55 to match the number of valid responses collected.

Evidence of the calculated sample size is given below in Figure 6.

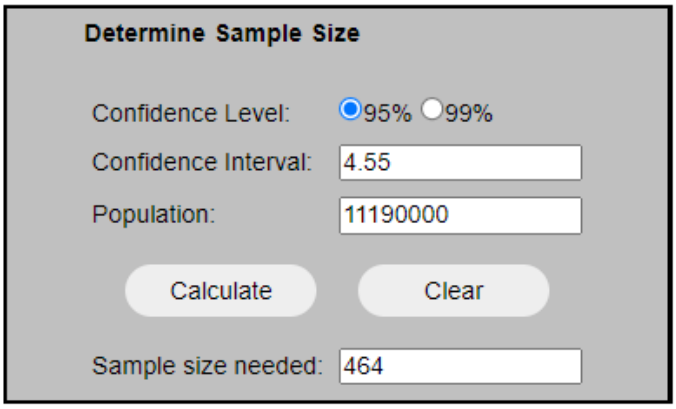


Figure 3.4: Sample size (source: Creative Research Systems, 2021)

3.5 Sample Method

Researchers generally use convenience samples to obtain a large number of completed questionnaires quickly and economically (Zikmund, Babin, Carr, & Giffin, 2013). Clear advantages of using convenience sampling are participants' availability and less time framework requirement to collect data for analysis (Cooksey, & McDonald, 2011; as cited by Kivunja, 2015). Data collected from a convenience sample allows the application of statistical knowledge covering how to work with missing data, significance interpretation, and effect size based on real data (Costanza, Blacksmith, & Coats, 2015). Therefore convenience sampling method is used in this research justified by the aforementioned citations.

3.6 Data Collection

A web-based SSS is used to collect responses from the target sample in this research. Furthermore, the Qualtrics platform is used to design and distribute the survey link accordingly. An anonymous link of the SSS is distributed among Facebook, WhatsApp, Messenger, Linkedin, Outlook, Yahoo, and Gmail platforms to reach the participants. This survey link is activated for seven weeks, from 22nd March to 3rd May, and is shared only after receiving approval from the Human Ethics in Research Group (HERG) of Waikato Institute of Technology (Wintec). Please find the detailed ethics form in Appendix D for more information. According to the information provided on the first page of the survey, all the responses are collected on a volunteering basis. There are 3 screening questions mentioned on the second page of the survey to filter the precise target respondents and record the valid responses from them.

3.7 Primary Data Description

653 responses are received from the survey and 76 participants have completed the survey partially. 43 responses become invalid from the aspects of the screening questions and 70 empty responses are recorded there as well. The final valid number of responses is calculated as 464 after omitting partially completed, empty, and other invalid responses.

3.8 Data Analysis Method

The data analysis activities are carried out based on the steps illustrated in Figure 3.5.

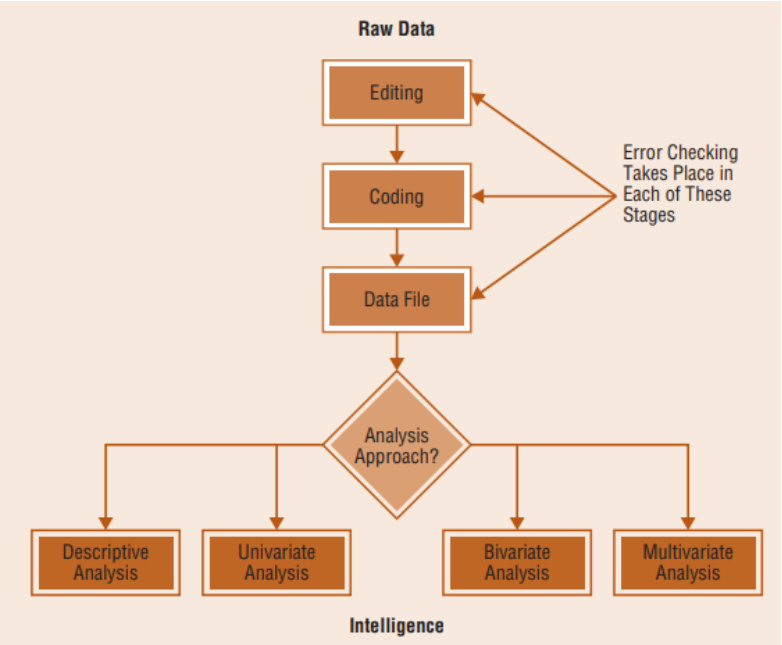


Figure 3.5: Overview of the Stages of Data Analysis (Sonquist & Dunkelberg, 1977; as Zikmund, Babin, Carr cited by, & Giffin, 2013)

Only descriptive analysis, univariate analysis, and bivariate analysis methods are considered in terms of this research. Further explanation of the above steps is done in subsections from 3.8.1 to 3.8.7 in the chapter.

3.8.1 Raw Data

The first step of the data analysis overview is collecting raw data. All 464 valid responses received for 22 survey questions in Qualtrics online survey tool are considered as raw data.

3.8.2 Editing

Editing action is the second step in the data analysis process. This step is taken place to reduce the unnecessary information in raw data. First, the raw data are exported to an SPSS formatted file from the Qualtrics tool. Then that file is uploaded to the SPSS software. Then the editing is done within the data set as required in the SPSS software.

3.8.3 Coding

The third step is coding that needs to perform before analyzing the data based on selected analysis methods. Each answer on the online survey is given a number based on their appearing order. That number is ranged from 1 – 8. Coding structures are presented from

Table B.1 – Table B.14 in Appendix B. This helps to present survey data in clear numeric figures. The researcher added labeling to each survey question for ease of reference in the SPSS software. These labels represent only the summary of the question as shown in Table B.15 in Appendix B. These labels are used when presenting chi-square test cross tabulation tables in Chapter 4.

3.8.4 Cronbach's Alpha

Instrument reliability is the main concern of questionnaire-based research. Cronbach's alpha is one of the popular reliability test applications that can be used in this matter (Rosli et al., 2016; Cunha et al., 2015; Fernández Batanero & Torres Gonzalez, 2015; Juned & Adil, 2015; as cited by Rosli et al., 2021). There are many views on the acceptable co-efficient value of Cronbach's alpha. A co-efficient of 0.5 or more is satisfactory (Helmstadter, 1964; as cited by Jones et al., 2020). Co-efficient value should ideally exceed 0.8 (Carmines & Zeller, 1979; Streiner & Norman, 1995; as cited by Jones et al., 2020). However, generally coefficient between 0.6 -0.7 is considered an acceptable level of reliability (Hulin, Netemeyer, and Cudeck, 2001; as cited by Ursachi, Horodnic, & Zait, 2015)

3.8.5 Descriptive Analysis

Descriptive statistics are used to summarize responses from a large pool of respondents in a few simple statistics (Zikmund et al., 2013). Data collected from SSS are visualized in frequency tables according to the type of responses received from survey participants under each survey question. All the survey questions are matched with the variables identified in the modified UTAUT model and thereby disclose the impact of each variable over the other based on the responses received accordingly.

3.8.6 Univariate Analysis: Chi-square

Pearson's Chi-square test of independence is used to identify the connection between two variables (McKechnie & Fisher, 2019). In the survey SQ1: Age, SQ2: Gender, and SQ3: Education level are independent variables. SQ5, SQ7, SQ9, SQ11, and SQ19 represent current cyber awareness while SQ6, SQ8, SQ10, SQ12, SQ13, SQ14, SQ15, SQ16, SQ17, SQ18, and SQ20 represent current cyber behavior respectively and both of them are median variables. SQ21 represents currently believed user cyber awareness and SQ22 represents currently believed user cyber behavior. All these independent and median variables are tested against relevant survey questions accordingly to prove hypotheses established in the research.

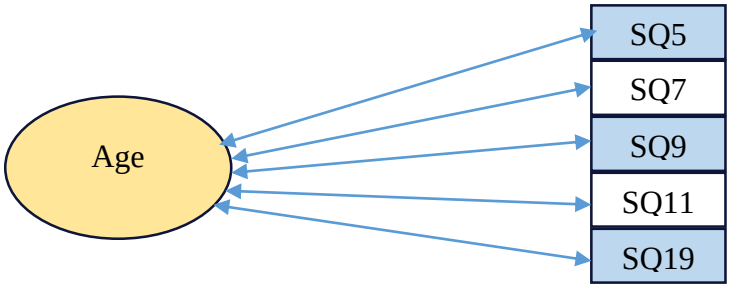


Figure 3.6 Chi-square category variables: Age and other survey questions

Table 3.4 Age, relevant survey questions, and related hypotheses for chi-square analysis

Independent variable	Survey question	H
Age	SQ5	H_1 - Age has no impact on the user's cyber awareness (SQ5) H_2- Age has an impact on the user's cyber awareness (SQ5)
	SQ7	H_1 - Age has no impact on the user's cyber awareness (SQ7) H_2- Age has an impact on the user's cyber awareness (SQ7)
	SQ9	H_1 - Age has no impact on the user's cyber awareness (SQ9) H_2- Age has an impact on the user's cyber awareness (SQ9)
	SQ11	H_1 - Age has no impact on the user's cyber awareness (SQ11) H_2- Age has an impact on the user's cyber awareness (SQ11)
	SQ19	H_1 - Age has no impact on the user's cyber awareness (SQ19) H_2- Age has an impact on the user's cyber awareness (SQ19)

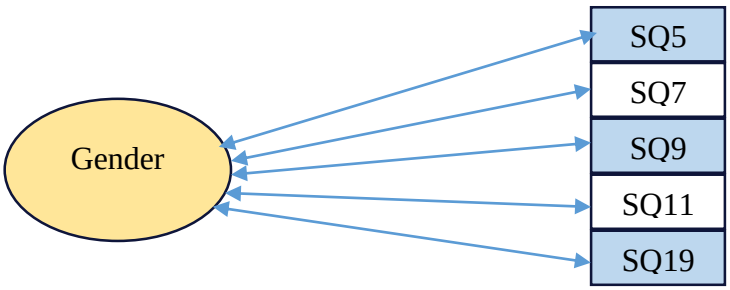


Figure 3.7: Chi-square category variables: Gender and other survey questions

Table 3.5 Gender, relevant survey questions, and related hypotheses for chi-square analysis

Independent variable	Survey question	H
Gender	SQ5	H_3 - Gender has no impact on the user's cyber awareness (SQ5) H_4- Gender has an impact on the user's cyber awareness (SQ5)
	SQ7	H_3 - Gender has no impact on the user's cyber awareness (SQ7) H_4- Gender has an impact on the user's cyber awareness (SQ7)
	SQ9	H_3 - Gender has no impact on the user's cyber awareness (SQ9) H_4- Gender has an impact on the user's cyber awareness (SQ9)
	SQ11	H_3 - Gender has no impact on the user's cyber awareness (SQ11) H_4- Gender has an impact on the user's cyber awareness (SQ11)
	SQ19	H_3 - Gender has no impact on the user's cyber awareness (SQ19) H_4- Gender has an impact on the user's cyber awareness (SQ19)

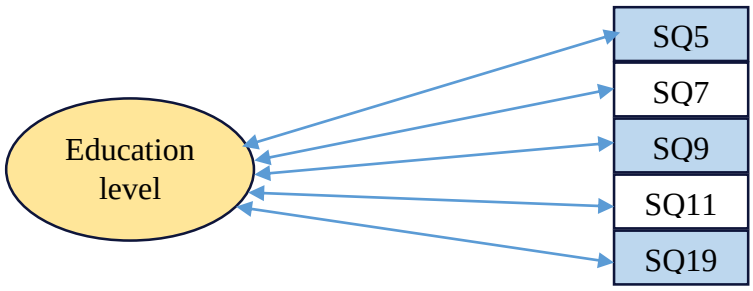


Figure 3.8: Chi-square category variables: Education level and other survey questions

Table 3.6 Education Level, relevant survey questions, and related hypotheses for chi-square analysis

Independent variable	Survey question	H
Education level	SQ5	H_5 - Education level has no impact on the user's cyber awareness (SQ5) H_6- Education level has an impact on the user's cyber awareness (SQ5)
	SQ7	H_5 - Education level has no impact on the user's cyber awareness (SQ7) H_6- Education level has an impact on the user's cyber awareness (SQ7)
	SQ9	H_5 - Education level has no impact on the user's cyber awareness (SQ9) H_6- Education level has an impact on the user's cyber awareness (SQ9)
	SQ11	H_5 - Education level has no impact on the user's cyber awareness (SQ11) H_6- Education level has an impact on the user's cyber awareness (SQ11)
	SQ19	H_5 - Education level has no impact on the user's cyber awareness (SQ19) H_6- Education level has an impact on the user's cyber awareness (SQ19)

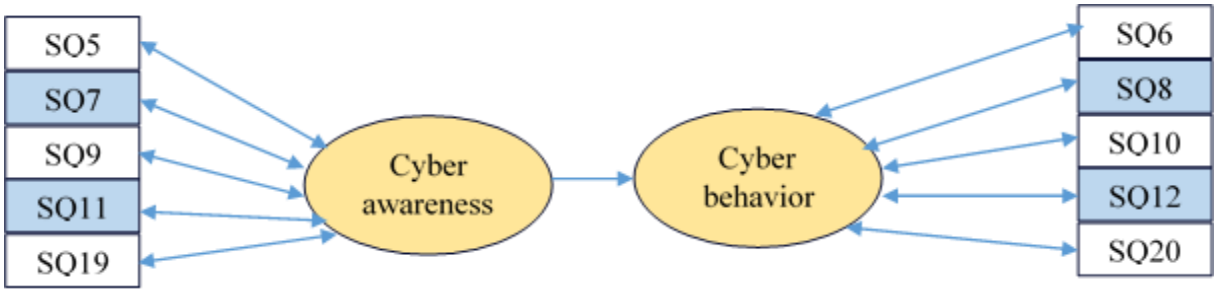


Figure 3.9 Chi-square category variables: cyber awareness, cyber behavior, and other survey question

Table 3.7 Cyber awareness, Cyber behavior, relevant survey questions and related hypotheses for chi-square analysis

Median variables	Survey question	H
Cyber awareness and cyber behavior	SQ5 and SQ6	H_7 - User's cyber awareness (SQ5) has no impact on the user's cyber behavior (SQ6) H_8- User's cyber awareness (SQ5) has an impact on the user's cyber behavior (SQ6)
	SQ7 and SQ8	H_7 - User's cyber awareness (SQ7) has no impact on the user's cyber behavior (SQ8) H_8- User's cyber awareness (SQ7) has an impact on the user's cyber behavior (SQ8)
	SQ9 and SQ10	H_7 - User's cyber awareness (SQ9) has no impact on the user's cyber behavior (SQ10) H_8- User's cyber awareness (SQ) has an impact on the user's cyber behavior (SQ10)
	SQ11 and S12	H_7 - User's cyber awareness (SQ11) has no impact on the user's cyber behavior (SQ12) H_8- User's cyber awareness (SQ11) has an impact on the user's cyber behavior (SQ12)
	SQ19 and SQ20	H_7 - User's cyber awareness (SQ19) has no impact on the user's cyber behavior (SQ20) H_8- User's cyber awareness (SQ19) has an impact on the user's cyber behavior (SQ20)

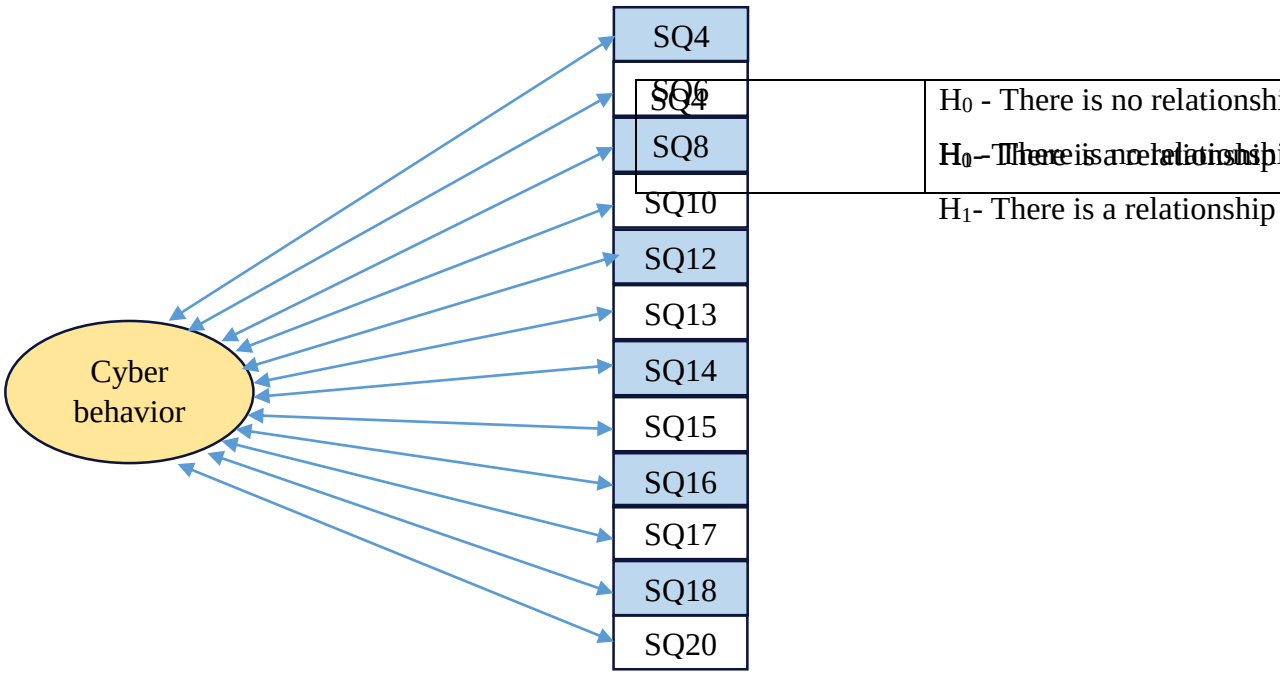


Figure 3.10: Chi-square category variables: cyber behavior and other survey questions

Table 3.8 Cyber behavior, relevant survey questions, and related hypotheses for chi-square analysis

Median variable	Survey question	H
Cyber behavior	SQ4	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ4) H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ4)
	SQ6	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ6) H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ6)

Median variable	Survey question	H
Cyber behavior	SQ8	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ8)
		H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ8)
	SQ10	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ10) H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ10)
	SQ12	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ12) H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ12)
	SQ13	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ13) H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ13)
	SQ14	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ14) H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ14)

Median variable	Survey question	H
Cyber behavior	SQ15	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ15) H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ15)
	SQ16	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ16) H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ16)
	SQ17	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ17) H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ17)
	SQ18	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ18) H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ18)
	SQ20	H_9 – User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform (SQ20) H_{10}- User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform (SQ20)

3.8.7 Bivariate Analysis: ANOVA

Analysis of variance (ANOVA) is a technique to evaluate combinations of several independent variables or factors. This analysis aims to identify those that have a significant effect on the value of a response variable (Tavakkolkhah, Zimmer, & Kuffner, 2018). ANOVA analysis is done considering three independent variables called age, gender, and education level in the research.

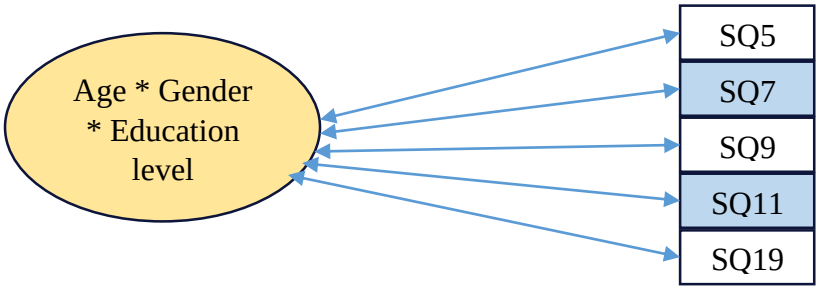


*Figure 3.11: ANOVA test age * gender* education level for main survey questions*

Table 3.9 Independent variables, relevant survey questions, and related hypotheses for ANOVA test

Independent variable	Survey question	H
Age * Gender * Education level	SQ5	H_0 – The interaction between age, gender, and education level does not affect cyber awareness H_1- The interaction between age, gender, and education level affects the cyber awareness
	SQ7	H_0 - The interaction between age, gender, and education level does not affect the cyber awareness H_1- The interaction between age, gender, and education level affects the cyber awareness
	SQ9	H_0 - The interaction between age, gender, and education level does not affect cyber awareness H_1- The interaction between age, gender, and education level affects the cyber awareness

Independent variable	Survey question	H
Age * Gender * Education level	SQ11	H_0 - The interaction between age, gender, and education level does not affect the cyber awareness H_1- The interaction between age, gender, and education level affects the cyber awareness
	SQ19	H_0 - The interaction between age, gender, and education level does not affect cyber awareness H_1- The interaction between age, gender, and education level affects the cyber awareness

3.9 Limitations of the Methodology

There are some limitations associated with the sampling method and data analysis methods. The population of interest is not represented by the sample, samples may not include variance on the variable of interest and numerous representative limitations in the samples are the three main concerns associated with convenience sampling (Landers & Behrend, 2015; as cited by Costanza et al., 2015). A convenience sample may not represent the population as a whole. Also, research-based on convenience sampling has limited external validity (Andrade, 2021). ANOVA analysis is based on two assumptions. The first one is that the values considered are normally distributed and the considering groups have the same variance (Tavakkolkhah et al., 2018).

3.10 Conclusion

The main RQ, sub-RQs, and H are established, a research framework is developed, data is collected from an online survey using convenience sampling and data analysis methods are identified and established in Chapter 3. The next chapter is focused on illustrating results generated from descriptive, univariate, and bivariate data analysis methods.

4. Results

4.1 Introduction

This chapter is presented with the results generated from various data analysis methods. Subsection 4.2.1 describes the reliability test results done using Cronbach's alpha. The results of data analysis based on descriptive analysis, univariate analysis: chi-square and bivariate analysis: three-way ANOVA methods are explained in subsections 4.2.2, 4.2.3, and 4.2.4 respectively. These data analysis results are generated using SPSS software in terms of tables and stacked charts. All the stacked charts relevant to descriptive analysis are explained in Appendix C accordingly. Finally, subsection 4.2.5 concludes chapter 4.

4.2 Data Analysis

This section is dedicated to present all the analysis results including Cronbach's alpha, descriptive analysis, chi-square analysis, and three-way ANOVA analysis.

4.2.1 Cronbach's Alpha

The purpose of calculating Cronbach's alpha co-efficiency in the research is to determine the reliability of the scale (Boyaci & Atalay, 2016). Therefore the researcher also used Cronbach's alpha to measure the Likert scale questions in the survey that consisted of 12 survey questions. Likert scale survey questions S5, S7, S9, S11, S19, and S21 are related to cyber awareness construct while Likert scale survey questions S6, S14, S15, S16, S18, and S22 are related to cyber behavior construct and thereby affects vulnerability construct as well. Please refer to Appendix A Survey questions for detailed information about the above Likert scale survey questions.

Table 4.1 Case processing summary

Case Processing Summary			
		N	%
Cases	Valid	464	100.0
	Excluded[a]	0	.0
	Total	464	100.0

As stated earlier, instrument reliability is the main concern of questionnaire-based research. Cronbach's alpha is one of the popular reliability test applications that can be used in this matter (Rosli et al., 2016; Cunha et al., 2015; Fernández Batanero & Torres Gonzalez, 2015;

Juned & Adil, 2015; as cited by Rosli et al., 2021). Generally, a coefficient between 0.6 -0.7 is considered an acceptable level of reliability (Hulin, Netemeyer, and Cudeck, 2001; as cited by Ursachi et al., 2015). As depicted in Table 4.2 the Cronbach's alpha value generated for the survey questions is 0.698 and it is within the acceptable level.

Table 4.2 Cronbach's alpha result

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.698	.693	12

4.2.2 Descriptive Analysis

As per Table 4.3 and Figure 4.1 majority of the survey participants are from age 25-34 representing 54.3% of the total participants. The second highest respondents are from age 35-44 showing 21.3%. The minimum number of participants is from age 65+ that is 2.8%.

Table 4.3 Age-wise distribution of survey participants

SQ1: Age					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18 - 24	60	12.9	12.9	12.9
	25 - 34	252	54.3	54.3	67.2
	35 - 44	99	21.3	21.3	88.6
	45 - 54	22	4.7	4.7	93.3
	55 - 64	18	3.9	3.9	97.2
	65+	13	2.8	2.8	100.0
	Total	464	100.0	100.0	

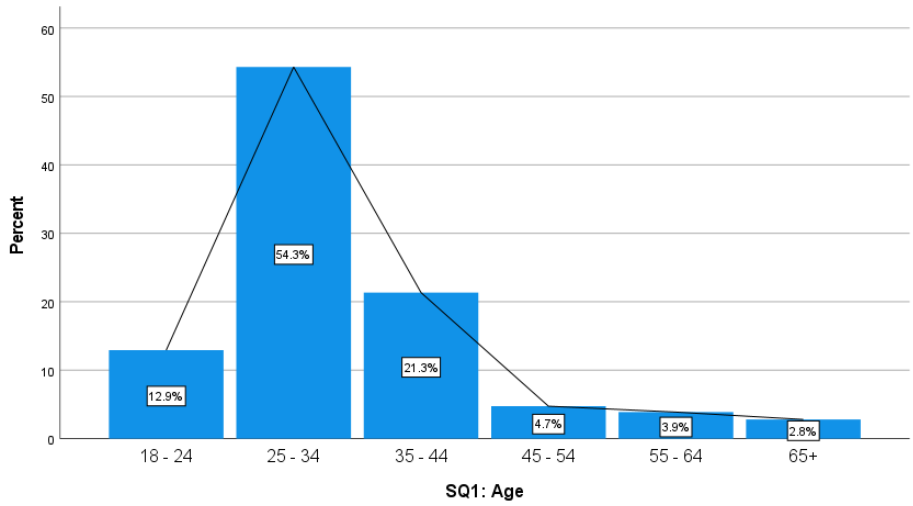


Figure 4.1: Age-wise distribution of survey participants

The gender distribution of the survey participants is illustrated in Table 4.4 and Figure 4.2. According to that 55.2% of the respondents are males and 44% of them are female. Only 1 respondent is from the “Other” category and 3 participants are from the “Prefer not to say” category.

Table 4.4 Gender wise distribution of survey participants

SQ2: Gender					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	256	55.2	55.2	55.2
	Female	204	44.0	44.0	99.1
	Other	1	.2	.2	99.4
	Prefer not to say	3	.6	.6	100.0
	Total	464	100.0	100.0	

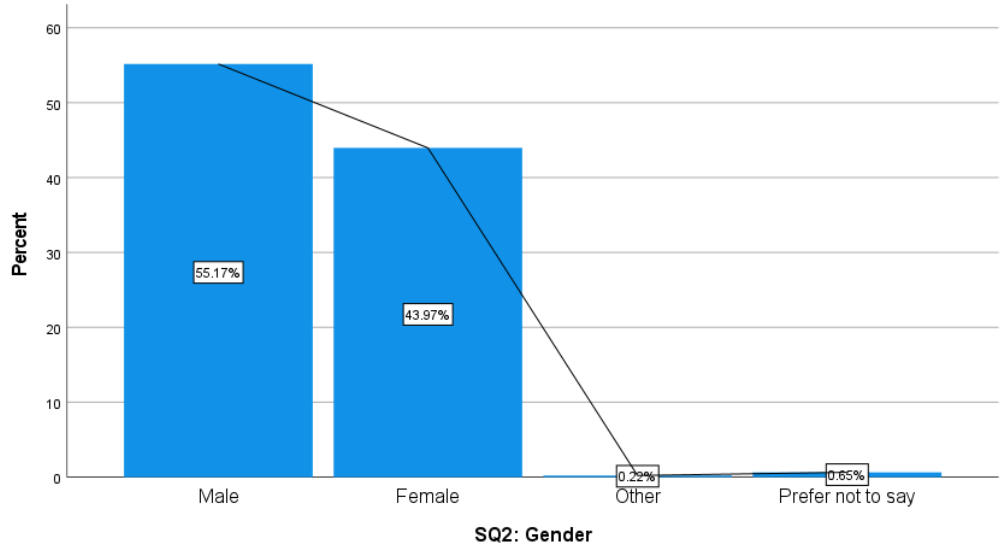


Figure 4.2: Gender wise distribution of survey participants

41% of the respondents are bachelor’s degree/graduate certificate or diploma holders as depicted in Table 4.5 and Figure 4.3. The next highest qualification gained by the respondents is a Master's degree with 16.6% followed by a Diploma level- 16.4%. There are only 2 people with doctoral degrees in the pool of respondents.

Table 4.5 Education level-wise distribution of survey participants

SQ3: Education level					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Secondary education	30	6.5	6.5	6.5
	Certificate Level	22	4.7	4.7	11.2
	Diploma Level	76	16.4	16.4	27.6
	Bachelor's Degree/ Graduate Certificate or Diploma	193	41.6	41.6	69.2
	Post Graduate Certificate/Diploma	64	13.8	13.8	83.0
	Master Degree	77	16.6	16.6	99.6
	Doctoral Degree	2	.4	.4	100.0
	Total	464	100.0	100.0	

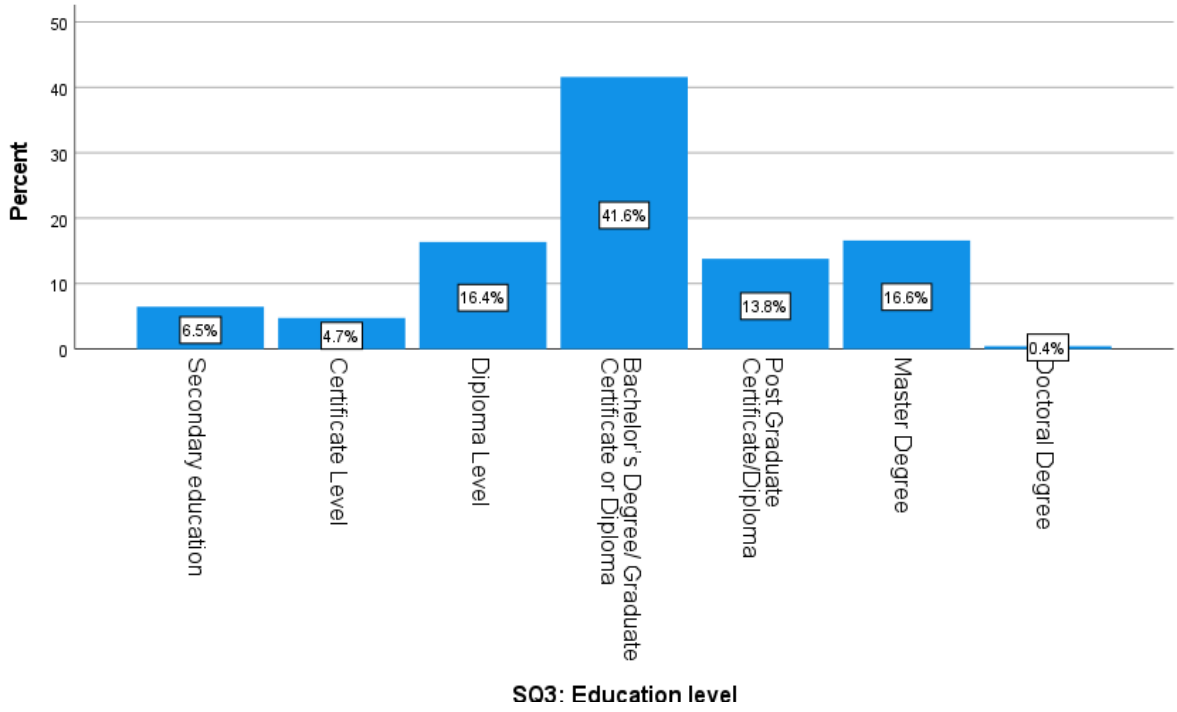


Figure 4.3: Education level-wise distribution of survey participants

Survey Question 4

42.7% of respondents are on Facebook for 0-3 hours weekly and 25.6% of them are using Facebook for 4-6 hours. Respondents who use Facebook 12+ hours weekly are less representing the lowest portion of total respondents as shown in Table 4.6. Age, gender, and education level-wise respondents distributions according to time spent on Facebook are illustrated in C.1, C.2, and C.3 Figures in Appendix C respectively.

Table 4.6 Time spent on Facebook

SQ4: Time spent on Facebook					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 - 3 hours	198	42.7	42.7	42.7
	4 - 6 hours	119	25.6	25.6	68.3
	7 - 9 hours	64	13.8	13.8	82.1
	10 – 12 hours	43	9.3	9.3	91.4
	12+ hours	40	8.6	8.6	100.0
	Total	464	100.0	100.0	

Survey Question 5

Table 4.7 depicts that 42.5% of respondents are aware of creating a strong password while 29.3% of them are moderately aware of that. Only 4.5% of them are not aware of this at all. C.4, C.5 and C.6 Figures in Appendix C depict more on age, gender, and education level-wise respondents distributions related to awareness of creating a strong password.

Table 4.7 Awareness of creating a strong password

SQ5: Awareness of creating a strong password					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Extremely aware	197	42.5	42.5	42.5
	Moderately aware	136	29.3	29.3	71.8
	Somewhat aware	81	17.5	17.5	89.2
	Slightly aware	29	6.3	6.3	95.5
	Not at all aware	21	4.5	4.5	100.0
	Total	464	100.0	100.0	

Survey Question 6

As illustrated in Table 4.8 38.8% of respondents are most likely to follow instructions provided by Facebook when creating the password while 40.3% of them are likely the follow the same instructions. Still, 5.8% unlikely and 2.2% most unlikely instruction followers are there among the pool of respondents. More information on age, gender, and education qualification level-wise respondents distribution for following instructions when creating the password is stated in C.7, C.8, and C.9 Figures in Appendix C accordingly.

Table 4.8 Follow instructions when creating the password

SQ6: Follow instructions when creating the password					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Most likely	180	38.8	38.8	38.8
	Likely	187	40.3	40.3	79.1
	Neutral	60	12.9	12.9	92.0
	Unlikely	27	5.8	5.8	97.8
	Most unlikely	10	2.2	2.2	100.0
	Total	464	100.0	100.0	

Survey Question 7

55.6% of respondents are extremely aware that the Facebook platform provides an option to set who can view their personal information in their profile while 23.3% of them moderately aware of that. As shown in Table 4.9, 4.3% are slightly aware of the option and 2.2% of them are not aware of it at all. Age, gender, and education level-wise distributions are further depicted in C.10, C.11, and C.12 Figures in Appendix C respectively.

Table 4.9 Awareness of personal information disclosure in profile

SQ7: Awareness of personal information disclosure in profile					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Extremely aware	258	55.6	55.6	55.6
	Moderately aware	108	23.3	23.3	78.9
	Somewhat aware	68	14.7	14.7	93.5
	Slightly aware	20	4.3	4.3	97.8
	Not at all aware	10	2.2	2.2	100.0
	Total	464	100.0	100.0	

Survey Question 8

As depicted in Table 4.10, 42.2% of respondents allow viewing their email/telephone number/address only for their selves. 36% of respondents allow them to view by friends while 4.1% of respondents do not know the current viewing of their email/telephone number/address. However, only 4.3% of respondents are aware that they can disregard entering email/telephone number/address in their profiles. C.13, C.14 and C.15 Figures in Appendix C further explain about age, gender, and education-wise distribution of respondents regarding current email/telephone number/address disclosure in their profiles.

Table 4.10 Current view of email/telephone number/address in the profile

SQ8: Currently view of email/telephone number/address in the profile					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Public	26	5.6	5.6	5.6
	Friends	167	36.0	36.0	41.6
	Close friends	32	6.9	6.9	48.5
	Acquaintances	1	.2	.2	48.7
	Friends except acquaintances	3	.6	.6	49.4
	Only me	196	42.2	42.2	91.6
	Do not know	19	4.1	4.1	95.7
	The email/telephone number/address is/are not entered in my profile	20	4.3	4.3	100.0
	Total	464	100.0	100.0	

Survey Question 9

As illustrated in Table 4.11, 40.5% of respondents are extremely aware of the two-factor authentication feature in Facebook. Still, 16.4% are not aware of that at all. Age, gender, and education level-wise respondents distribution related to awareness of personal information disclosure in the profile are further explained in C.16, C.17, and C.18 Figures in appendix C.

Table 4.11 Awareness of two-factor authentication

SQ9: Awareness of two-factor authentication					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Extremely aware	188	40.5	40.5	40.5
	Moderately aware	98	21.1	21.1	61.6
	Somewhat aware	59	12.7	12.7	74.4
	Slightly aware	43	9.3	9.3	83.6
	Not at all aware	76	16.4	16.4	100.0
	Total	464	100.0	100.0	

Survey Question 10

According to Table 4.12, the Majority of the respondents are not using two-factor authentication representing 59.1% of the total respondents. C.19, C.20, and C.21 Figures in Appendix C explain the age, gender, and education level-wise respondent distributions related to the use of two-factor authentication accordingly.

Table 4.12 Use of two-factor authentication

S10: Use of two-factor authentication					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	190	40.9	40.9	40.9
	No	274	59.1	59.1	100.0
	Total	464	100.0	100.0	

Survey Question 11

As illustrated in Table 4.13 43.3% of respondents are aware of the option on Facebook for setting up who can send friend requests and 10.8% of the respondents are not aware of this option at all. Further explanation on age, gender, and education level-wise respondent distributions related to this option are available in C.22, C.23, and C24 Figures in Appendix C respectively.

Table 4.13 Awareness of setting up who can send friend requests

SQ11: Awareness of setting up who can send friend requests					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Extremely aware	201	43.3	43.3	43.3
	Moderately aware	115	24.8	24.8	68.1
	Somewhat aware	69	14.9	14.9	83.0
	Slightly aware	29	6.3	6.3	89.2
	Not at all aware	50	10.8	10.8	100.0
	Total	464	100.0	100.0	

Survey Question 12

Only 51.5% of respondents use the option of who can send friend requests to their Facebook profile while 48.5% of respondents do not use the feature at all as shown in Table 4.14. Further clarification on age, gender, and education level-wise respondent distributions are in Figures C.25, C.26, and C.27 in appendix C respectively.

Table 4.14 Use of setting up who can send friend requests feature

SQ12: Use of setting up who can send friend requests feature					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	239	51.5	51.5	51.5
	No	225	48.5	48.5	100.0
	Total	464	100.0	100.0	

Survey Question 13

As illustrated in Table 4.15, only 5% of respondents check and update privacy and security settings once a week and only 19.8% are doing it once a month. The majority of the

respondents check and update the privacy and security settings once in a quarter or once a year or never. Age, gender, and education level-wise distributions of respondents with this regard are elaborated in Figures C.28, C.29, and C.30 in appendix C respectively.

Table 4.15 Check and update the privacy and security settings

SQ13: Check and update the privacy and security settings					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Once a week	23	5.0	5.0	5.0
	Once a month	92	19.8	19.8	24.8
	Once in a quarter	114	24.6	24.6	49.4
	Once a year	105	22.6	22.6	72.0
	Never	130	28.0	28.0	100.0
	Total	464	100.0	100.0	

Survey Question 14

As depicts in Table 4.16 majority of respondents never accept friend requests from unknown people that consist 52.4%. A small number of respondents representing 1.3% always accept friend requests from unknown people. C.31, C.32 and C.33 Figures in Appendix C elaborates on age, gender, and education level-wise respondent distribution related to this matter respectively.

Table 4.16 Accept friend requests

SQ14: Accept friend requests					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	6	1.3	1.3	1.3
	Sometimes	87	18.8	18.8	20.0
	Rarely	128	27.6	27.6	47.6
	Never	243	52.4	52.4	100.0
	Total	464	100.0	100.0	

Survey Question 15

64.2% of survey participants never send friend requests to unknown people as illustrated in Table 4.17. Only 1.1% of survey participants always send friend requests to unknown people and it is comparatively a small amount. Age, gender, and education level-wise detailed distribution of survey participants related to sending friend requests are presented in C.34, C.35, and C.36 Figures in Appendix C respectively.

Table 4.17 Send friend requests

SQ15: Send friend requests					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	5	1.1	1.1	1.1
	Sometimes	72	15.5	15.5	16.6
	Rarely	89	19.2	19.2	35.8
	Never	298	64.2	64.2	100.0
	Total	464	100.0	100.0	

Survey Question 16

Table 4.18 elaborates that only 3.2% of respondents are most likely to click any link that comes to their profile before verifying it. On the other hand, the majority consisting of 38.4% of respondents are most unlikely to click any link before verifying it. C.37, C.38 and C.39 Figures in Appendix C elaborates on age, gender, and education level-wise respondent distribution with regards to clicking unknown links accordingly.

Table 4.18 Clicking unknown links

SQ16: Clicking unknown links					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Most likely	15	3.2	3.2	3.2
	Likely	46	9.9	9.9	13.1
	Neutral	82	17.7	17.7	30.8
	Unlikely	143	30.8	30.8	61.6
	Most unlikely	178	38.4	38.4	100.0
	Total	464	100.0	100.0	

Survey Question 17

43.5% of survey participants are never changing their password on Facebook while only 4.1% of them change it once a month as shown in Table 4.19. Age, gender, and education level-wise participant distributions related to this question are further clarified in C.40, C.41, and C.42 Figures in Appendix C respectively.

Table 4.19 Password change frequency on Facebook

SQ17: Password change frequency					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Once a month	19	4.1	4.1	4.1
	Once in a quarter	45	9.7	9.7	13.8
	Once in six months	64	13.8	13.8	27.6
	Once a year	134	28.9	28.9	56.5
	Never	202	43.5	43.5	100.0
	Total	464	100.0	100.0	

Survey Question 18

As elaborated in Table 4.20, 30% of respondents are most likely to log out from their profile on any device when they no longer use it. 22.8% of respondents are likely to follow this practice. On the other hand, 16.2% of respondents are unlikely and 15.1% of respondents are most unlikely to follow this practice. C.43, C.44, and C.45 Figures in Appendix C explain this practice more based on age, gender, and education level respectively.

Table 4.20 Logging out from devices after using Facebook

SQ18: Logging out after use					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Most likely	139	30.0	30.0	30.0
	Likely	106	22.8	22.8	52.8
	Neutral	74	15.9	15.9	68.8
	Unlikely	75	16.2	16.2	84.9
	Most unlikely	70	15.1	15.1	100.0
	Total	464	100.0	100.0	

Survey Question 19

According to Table 4.21, 35.8% of participants are likely and 41.8% most likely consider the security of what they share on Facebook. However, only 6.7% of participants are unlikely and 2.8% of participants are most unlikely to consider security when they share photos, videos, and posts on Facebook. Age, gender, and education qualification-wise participant distribution are illustrated in Figures C.46, C.47, and C.48 in appendix C in detail with this regard respectively.

Table 4.21 Consideration of security before sharing photos, videos, and posts on Facebook

S19: Consideration of security before sharing photos, videos and posts					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Most likely	194	41.8	41.8	41.8
	Likely	166	35.8	35.8	77.6
	Neutral	60	12.9	12.9	90.5
	Unlikely	31	6.7	6.7	97.2
	Most unlikely	13	2.8	2.8	100.0
	Total	464	100.0	100.0	

Survey Question 20

As shown in Table 4.21 majority of respondents have shared photos, videos, and posts among friends representing 72.1% of the pool of respondents. 14.6% of respondents are shared those in public. Multiple responses are allowed for this question. However, this question is not feasible to illustrate in stacked bar charts based on age, gender, and education level wise as this consists of multiple answers.

Table 4.22 Current view photos, videos, and posts on Facebook

Current view Of photos, videos and posts frequencies				
		Responses		Percent of Cases
		N	Percent	
Current view of photos, videos, and Posts	S20_1_Current view photos, videos and posts: Public	77	14.6%	16.6%
	S20_2_Current view photos, videos and posts: Friends	379	72.1%	81.9%
	S20_3_Current view photos, videos and posts: Close friends	43	8.2%	9.3%
	S20_4_Current view photos, videos and posts: Acquaintances	6	1.1%	1.3%
	S20_5_Current view photos, videos and posts: Friends except acquaintances	8	1.5%	1.7%
	S20_6_Current view photos, videos and posts: Only me	13	2.5%	2.8%
Total		526	100.0%	113.6%

Survey Question 21

The majority of the participants are believing that they have a moderate level of awareness regarding cyber threats on Facebook representing 55.6% of the total pool of respondents as illustrated in Table 4.23. Only 4.3% of participants are believing that they are not aware at all in this regard. Age, gender, and education level-wise participant distributions are further illustrated in Figures C.49, C.50, and C.51 in appendix C respectively related to this survey question.

Table 4.23 Current view photos, videos, and posts on Facebook

SQ21: Current believed awareness level of user					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strong level of awareness	109	23.5	23.5	23.5
	Moderate level of awareness	258	55.6	55.6	79.1
	A lower level of awareness	75	16.2	16.2	95.3
	No awareness at all	22	4.7	4.7	100.0
	Total	464	100.0	100.0	

Survey Question 22

As depicted in Table, 4.24, 60.6% of respondents are either agree or strongly agree on the question regarding the belief they have taken enough precautions to safeguard their Facebook profile from cyber threats. Only 11.8% of the respondents either disagree or strongly disagree with this regard. More clarification on age, gender, and education-wise respondent distributions are shown in Figures C.52, C.53, and C.54 in appendix C related to this question accordingly.

Table 4.24 Current view photos, videos, and posts on Facebook

SQ22: Current believed behavior level of the user					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly agree	69	14.9	14.9	14.9
	Agree	212	45.7	45.7	60.6
	Neither agree or disagree	128	27.6	27.6	88.1
	disagree	48	10.3	10.3	98.5
	Strongly disagree	7	1.5	1.5	100.0
	Total	464	100.0	100.0	

4.2.3 Univariate Analysis: Chi-Square

The chi-square test is mainly used to identify the impact of independent variables over median variables and median variables over the dependent variable in this research. First, the impact of three independent variables (age, gender, and education level) are measured over cyber awareness. Then the impact of cyber awareness is measured over cyber behavior. Finally, the impact of actual cyber behavior is measured over the current believed behavior to identify the vulnerability level of Facebook users.

Analysis of Age and other survey questions

Age* SQ5

H_1 – Age has no impact on the user's cyber awareness

H_2 – Age has an impact on the user's cyber awareness

Table 4.25 Number of respondents answered to SQ5

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ1: Age * SQ5: Awareness of creating a strong password	464	100.0%	0	0.0%	464	100.0%

Table 4.26 Cross-tabulation Age * SQ5

SQ1: Age * SQ5: Awareness of creating a strong password Cross tabulation							
		SQ5: Awareness of creating a strong password					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ1: Age	18 - 24	29	14	10	5	2	60
	25 - 34	126	64	42	12	8	252
	35 - 44	35	34	19	4	7	99
	45 - 54	5	6	4	4	3	22
	55 - 64	2	10	4	1	1	18
	65+	0	8	2	3	0	13
Total		197	136	81	29	21	464

Table 4.27 Chi-square result for Age * SQ5

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	49.355[a]	20	.000
Likelihood Ratio	50.054	20	.000
Linear-by-Linear Association	14.404	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between age and cyber awareness (SQ5) based on the above results. Therefore,

H_2: Age has an impact on the user's cyber awareness

Also, participants from age 18 -34 have comparatively more moderated awareness (above 70%) than participants from age 35- 65+ according to the above results.

Age * SQ7

H_1 – Age has no impact on the user's cyber awareness

H_2 – Age has an impact on the user's cyber awareness

Table 4.28 Number of respondents answered to SQ7

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ1: Age * SQ7: Awareness of personal information disclosure in profile	464	100.0%	0	0.0%	464	100.0%

Table 4.29 Cross-tabulation Age * SQ7

SQ1: Age * SQ7: Awareness of personal information disclosure in profile Cross tabulation							
		SQ7: Awareness of personal information disclosure in profile					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ1: Age	18 - 24	30	18	8	1	3	60
	25 - 34	159	52	31	7	3	252
	35 - 44	57	25	12	3	2	99
	45 - 54	7	7	5	2	1	22
	55 - 64	4	2	7	5	0	18
	65+	1	4	5	2	1	13
Total		258	108	68	20	10	464

Table 4.30 Chi-square result for Age * SQ7

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	69.831[a]	20	.000
Likelihood Ratio	55.610	20	.000
Linear-by-Linear Association	26.500	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between age and cyber awareness (SQ7) based on the above results.

So it is identified that,

H_2: Age has an impact on the user's cyber awareness

Also, participants from age 18 -44 have comparatively more moderate awareness (above 80%) than participants from age 45- 65+ according to the above results.

Age * SQ9

H_1 – Age has no impact on the user's cyber awareness

H_2 – Age has an impact on the user's cyber awareness

Table 4.31 Number of respondents answered to SQ9

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ1: Age * SQ9: Awareness of two-factor authentication	464	100.0%	0	0.0%	464	100.0%

Table 4.32 Cross-tabulation Age * SQ9

SQ1: Age * SQ9: Awareness of two-factor authentication Cross tabulation							
		SQ9: Awareness of two-factor authentication					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ1: Age	18 - 24	19	16	8	6	11	60
	25 - 34	125	52	34	14	27	252
	35 - 44	35	25	10	15	14	99
	45 - 54	7	0	2	3	10	22
	55 - 64	2	2	4	2	8	18
	65+	0	3	1	3	6	13
Total		188	98	59	43	76	464

Table 4.33 Chi-square result for Age * SQ9

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	69.227[a]	20	.000
Likelihood Ratio	71.472	20	.000
Linear-by-Linear Association	29.960	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between age and cyber awareness (SQ9) based on the above results. Hence,

H_2: Age has an impact on the user's cyber awareness

Also, participants from age 25 -44 have comparatively more moderate awareness (above 70%) than participants from age 18-24 and age 45- 65+ according to the above results.

Age * SQ11

H_1 – Age has no impact on the user's cyber awareness

H_2 – Age has an impact on the user's cyber awareness

Table 4.34 Number of respondents answered to SQ11

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ1: Age * SQ11: Awareness of setting up who can send friend requests	464	100.0%	0	0.0%	464	100.0%

Table 4.35 Cross-tabulation Age * SQ11

SQ1: Age * SQ11: Awareness of setting up who can send friend requests Cross tabulation							
		SQ11: Awareness of setting up who can send friend requests					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ1: Age	18 - 24	27	20	6	0	7	60
	25 - 34	129	60	33	9	21	252
	35 - 44	33	28	17	9	12	99
	45 - 54	7	3	3	4	5	22
	55 - 64	4	1	5	4	4	18
	65+	1	3	5	3	1	13
Total		201	115	69	29	50	464

Table 4.36 Chi-square result for Age * SQ11

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	60.154[a]	20	.000
Likelihood Ratio	58.037	20	.000
Linear-by-Linear Association	26.666	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between age and cyber awareness (SQ11) based on the above results. Therefore,

H_2: Age has an impact on the user's cyber awareness

Also, participants from age 18 -34 have comparatively more moderate awareness (above 75%) than participants from age 45- 65+ according to the above results.

Age * SQ19

H_1 – Age has no impact on the user's cyber awareness

H_2 – Age has an impact on the user's cyber awareness

Table 4.37 Number of respondents answered to SQ19

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ1: Age * S19: Consideration of security before sharing photos, videos and posts	464	100.0%	0	0.0%	464	100.0%

Table 4.38 Cross-tabulation Age * SQ19

SQ1: Age * S19: Consideration of security before sharing photos, videos and posts Cross tabulation							
		S19: Consideration of security before sharing photos, videos and posts					Total
		Most likely	Likely	Neutral	Unlikely	Most unlikely	
SQ1: Age	18 - 24	23	24	9	2	2	60
	25 - 34	110	92	28	16	6	252
	35 - 44	47	29	14	7	2	99
	45 - 54	7	9	4	1	1	22
	55 - 64	3	8	3	2	2	18
	65+	4	4	2	3	0	13
Total		194	166	60	31	13	464

Table 4.39 Chi-square result for Age * SQ19

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	21.030[a]	20	.395
Likelihood Ratio	18.422	20	.560
Linear-by-Linear Association	5.158	1	.023
N of Valid Cases	464		

p=0.395

p>0.05

There is no relationship between age and cyber awareness (SQ19) based on the above results.

So,

H_1: Age has no impact on the user's cyber awareness

Gender * SQ5

H_3 – Gender has no impact on the user's cyber awareness

H_4 – Gender has an impact on the user's cyber awareness

Table 4.40 Number of respondents answered to SQ5

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ2: Gender * SQ5: Awareness of creating a strong password	464	100.0%	0	0.0%	464	100.0%

Table 4.41 Cross-tabulation Gender * SQ5

SQ2: Gender * SQ5: Awareness of creating a strong password Cross tabulation							
		SQ5: Awareness of creating a strong password					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ2: Gender	Male	105	81	42	16	12	256
	Female	90	54	39	12	9	204
	Other	1	0	0	0	0	1
	Prefer not to say	1	1	0	1	0	3
Total		197	136	81	29	21	464

Table 4.42 Chi-square result for Gender * SQ5

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7.453[a]	12	.826
Likelihood Ratio	6.678	12	.878
Linear-by-Linear Association	.010	1	.920
N of Valid Cases	464		

p=0.826

p>0.05

There is no relationship between gender and cyber awareness (SQ5) based on the above results. Hence,

H_3: Gender has no impact on the user's cyber awareness

Gender * SQ7

H_3 – Gender has no impact on the user's cyber awareness

H_4 – Gender has an impact on the user's cyber awareness

Table 4.43 Number of respondents answered to SQ7

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ2: Gender * SQ7: Awareness of personal information disclosure in profile	464	100.0%	0	0.0%	464	100.0%

Table 4.44 Cross-tabulation Gender * SQ7

SQ2: Gender * SQ7: Awareness of personal information disclosure in profile Cross tabulation							
		SQ7: Awareness of personal information disclosure in profile					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ2: Gender	Male	136	64	43	8	5	256
	Female	118	44	25	12	5	204
	Other	1	0	0	0	0	1
	Prefer not to say	3	0	0	0	0	3
Total		258	108	68	20	10	464

Table 4.45 Chi-square result for Gender * SQ7

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7.982[a]	12	.787
Likelihood Ratio	9.462	12	.663
Linear-by-Linear Association	.649	1	.420
N of Valid Cases	464		

p=0.787

p>0.05

There is no relationship between gender and cyber awareness (SQ7) based on the above results. Therefore,

H_3: Gender has no impact on the user's cyber awareness

Gender * SQ9

H_3 – Gender has no impact on the user's cyber awareness

H_4 – Gender has an impact on the user's cyber awareness

Table 4.46 Number of respondents answered to SQ9

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ2: Gender * SQ9: Awareness of two-factor authentication	464	100.0%	0	0.0%	464	100.0%

Table 4.47 Cross-tabulation Gender * SQ9

SQ2: Gender * SQ9: Awareness of two-factor authentication Cross tabulation							
		SQ9: Awareness of two-factor authentication					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ2: Gender	Male	107	68	31	17	33	256
	Female	79	29	27	26	43	204
	Other	1	0	0	0	0	1
	Prefer not to say	1	1	1	0	0	3
Total		188	98	59	43	76	464

Table 4.48 Chi-square result for Gender * SQ9

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	21.288[a]	12	.046
Likelihood Ratio	22.237	12	.035
Linear-by-Linear Association	5.662	1	.017
N of Valid Cases	464		

p=0.046

p<0.05

There is a relationship between gender and cyber awareness (SQ9) based on the above results. So,

H_4: Gender has an impact on the user's cyber awareness

Also, male participants have comparatively more moderate awareness (approximately 68%) than female participants (approximately 53%) according to the above results.

Gender * SQ11

H_3 – Gender has no impact on the user's cyber awareness

H_4 – Gender has an impact on the user's cyber awareness

Table 4.49 Number of respondents answered to SQ11

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ2: Gender * SQ11: Awareness of setting up who can send friend requests	464	100.0%	0	0.0%	464	100.0%

Table 4.50 Cross-tabulation Age * SQ11

SQ2: Gender * SQ11: Awareness of setting up who can send friend requests Cross tabulation							
		SQ11: Awareness of setting up who can send friend requests					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ2: Gender	Male	102	76	39	13	26	256
	Female	97	38	30	15	24	204
	Other	1	0	0	0	0	1
	Prefer not to say	1	1	0	1	0	3
Total		201	115	69	29	50	464

Table 4.51 Chi-square result for Age * SQ11

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	14.178[a]	12	.289
Likelihood Ratio	13.666	12	.323
Linear-by-Linear Association	.003	1	.960
N of Valid Cases	464		

p=0.289

p>0.05

There is no relationship between gender and cyber awareness (SQ11) based on the above results. Hence,

H_3: Gender has no impact on the user's cyber awareness

Gender * SQ19

H_3 – Gender has no impact on the user's cyber awareness

H_4 – Gender has an impact on the user's cyber awareness

Table 4.52 Number of respondents answered to SQ19

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ2: Gender * S19: Consideration of security before sharing photos, videos and posts	464	100.0%	0	0.0%	464	100.0%

Table 4.53 Cross-tabulation Gender * SQ19

SQ2: Gender * S19: Consideration of security before sharing photos, videos and posts Cross tabulation							
		S19: Consideration of security before sharing photos, videos and posts					Total
		Most likely	Likely	Neutral	Unlikely	Most unlikely	
SQ2: Gender	Male	94	95	37	21	9	256
	Female	98	70	22	10	4	204
	Other	0	0	1	0	0	1
	Prefer not to say	2	1	0	0	0	3
Total		194	166	60	31	13	464

Table 4.54 Chi-square result for Gender * SQ19

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	15.604[a]	12	.210
Likelihood Ratio	13.639	12	.324
Linear-by-Linear Association	7.427	1	.006
N of Valid Cases	464		

p=0.210

p>0.05

There is no relationship between gender and cyber awareness (SQ19) based on the above results. Therefore,

H_3: Gender has no impact on the user's cyber awareness

Education level * SQ5

H_5 – Education level has no impact on the user's cyber awareness

H_6 – Education level has an impact on the user's cyber awareness

Table 4.55 Number of respondents answered to SQ5

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ3: Education level * SQ5: Awareness of creating a strong password	464	100.0%	0	0.0%	464	100.0%

Table 4.56 Cross-tabulation Education level * SQ5

SQ3: Education level * SQ5: Awareness of creating a strong password Cross tabulation							
		SQ5: Awareness of creating a strong password					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ3: Education level	Secondary education	18	6	5	0	1	30
	Certificate Level	10	9	1	2	0	22
	Diploma Level	31	19	13	8	5	76
	Bachelor's Degree/ Graduate Certificate or Diploma	74	61	36	11	11	193
	Post Graduate Certificate/Diploma	28	17	13	2	4	64
	Master Degree	36	23	13	5	0	77
	Doctoral Degree	0	1	0	1	0	2
Total		197	136	81	29	21	464

Table 4.57 Chi-square result for Education level * SQ5

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	28.368[a]	24	.245
Likelihood Ratio	32.547	24	.114
Linear-by-Linear Association	.059	1	.807
N of Valid Cases	464		

p=0.245

p>0.05

There is no relationship between education level and cyber awareness (SQ5) based on the above results. So,

H_5: Education level has no impact on the user's cyber awareness

Education level * SQ7

H_5 – Education level has no impact on the user's cyber awareness

H_6 – Education level has an impact on the user's cyber awareness

Table 4.58 Number of respondents answered to SQ7

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ3: Education level * SQ7: Awareness of personal information disclosure in profile	464	100.0%	0	0.0%	464	100.0%

Table 4.59 Cross-tabulation Education level * SQ7

SQ3: Education level * SQ7: Awareness of personal information disclosure in profile Cross tabulation							
		SQ7: Awareness of personal information disclosure in profile					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ3: Education level	Secondary education	18	7	3	1	1	30
	Certificate Level	11	4	4	2	1	22
	Diploma Level	35	14	19	5	3	76
	Bachelor's Degree/ Graduate Certificate or Diploma	113	47	24	5	4	193
	Post Graduate Certificate/Diploma	35	16	9	3	1	64
	Master Degree	46	19	8	4	0	77
	Doctoral Degree	0	1	1	0	0	2
Total		258	108	68	20	10	464

Table 4.60 Chi-square result for Education level * SQ7

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	21.945[a]	24	.583
Likelihood Ratio	22.804	24	.531
Linear-by-Linear Association	2.275	1	.131
N of Valid Cases	464		

p=0.583

p>0.05

There is no relationship between education level and cyber awareness (SQ7) based on the above results. Hence,

H_5: Education level has no impact on the user's cyber awareness

Education level * SQ9

H_5 – Education level has no impact on the user's cyber awareness

H_6 – Education level has an impact on the user's cyber awareness

Table 4.61 Number of respondents answered to SQ9

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ3: Education level * SQ9: Awareness of two-factor authentication	464	100.0%	0	0.0%	464	100.0%

Table 4.62 Cross-tabulation Education level * SQ9

SQ3: Education level * SQ9: Awareness of two-factor authentication Cross tabulation							
		SQ9: Awareness of two-factor authentication					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ3: Education level	Secondary education	14	6	3	3	4	30
	Certificate Level	3	5	6	3	5	22
	Diploma Level	23	19	13	5	16	76
	Bachelor's Degree/ Graduate Certificate or Diploma	88	42	23	15	25	193
	Post Graduate Certificate/Diploma	24	15	5	6	14	64
	Master Degree	36	11	8	10	12	77
	Doctoral Degree	0	0	1	1	0	2
Total		188	98	59	43	76	464

Table 4.63 Chi-square result for Education level * SQ9

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	31.727[a]	24	.134
Likelihood Ratio	31.137	24	.150
Linear-by-Linear Association	.279	1	.598
N of Valid Cases	464		

p=0.134

p>0.05

There is no relationship between education level and cyber awareness (SQ9) based on the above results. Therefore,

H_5: Education level has no impact on the user's cyber awareness

Education level * SQ11

H_5 – Education level has no impact on the user's cyber awareness

H_6 – Education level has an impact on the user's cyber awareness

Table 4.64 Number of respondents answered to SQ11

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ3: Education level * SQ11: Awareness of setting up who can send friend requests	464	100.0%	0	0.0%	464	100.0%

Table 4.65 Cross-tabulation Education level * SQ11

SQ3: Education level * SQ11: Awareness of setting up who can send friend requests Cross tabulation							
		SQ11: Awareness of setting up who can send friend requests					Total
		Extremely aware	Moderately aware	Somewhat aware	Slightly aware	Not at all aware	
SQ3: Education level	Secondary education	14	9	2	1	4	30
	Certificate Level	3	9	3	2	5	22
	Diploma Level	29	17	17	8	5	76
	Bachelor's Degree/ Graduate Certificate or Diploma	92	46	29	8	18	193
	Post Graduate Certificate/Diploma	22	18	10	4	10	64
	Master Degree	41	15	8	5	8	77
	Doctoral Degree	0	1	0	1	0	2
Total		201	115	69	29	50	464

Table 4.66 Chi-square result for Education level * SQ11

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	36.599[a]	24	.048
Likelihood Ratio	34.684	24	.073
Linear-by-Linear Association	.668	1	.414
N of Valid Cases	464		

p=0.048

p<0.05

There is a relationship between education level and cyber awareness (SQ11) based on the above results. So,

H_6: Education level has an impact on the user's cyber awareness

Education level * SQ19

H_5 – Education level has no impact on the user's cyber awareness

H_6 – Education level has an impact on the user's cyber awareness

Table 4.67 Number of respondents answered to SQ19

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ3: Education level * S19: Consideration of security before sharing photos, videos and posts	464	100.0%	0	0.0%	464	100.0%

Table 4.68 Cross-tabulation Education level * SQ19

SQ3: Education level * S19: Consideration of security before sharing photos, videos and posts Cross tabulation							
		S19: Consideration of security before sharing photos, videos and posts					Total
		Most likely	Likely	Neutral	Unlikely	Most unlikely	
SQ3: Education level	Secondary education	12	13	4	1	0	30
	Certificate Level	5	7	4	3	3	22
	Diploma Level	24	34	12	5	1	76
	Bachelor's Degree/ Graduate Certificate or Diploma	97	60	23	8	5	193
	Post Graduate Certificate/Diploma	20	28	8	5	3	64
	Master Degree	36	23	9	8	1	77
	Doctoral Degree	0	1	0	1	0	2
Total		194	166	60	31	13	464

Table 4.69 Chi-square result for Education level * SQ19

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	40.523[a]	24	.019
Likelihood Ratio	34.953	24	.069
Linear-by-Linear Association	.193	1	.660
N of Valid Cases	464		

p=0.019

p<0.05

There is a relationship between education level and cyber awareness (SQ19) based on the above results. Hence,

H_6: Education level has an impact on the user's cyber awareness

User's cyber awareness (SQ5) * user's cyber behavior (SQ6)

H_7 – User's cyber awareness has no impact on the user's cyber behavior

H_8 – User's cyber awareness has an impact on the user's cyber behavior

Table 4.70 Number of respondents answered to SQ5 and SQ6

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ5: Awareness of creating a strong password * SQ6: Follow instructions when creating the password	464	100.0%	0	0.0%	464	100.0%

Table 4.71 Cross-tabulation actual awareness (SQ5) * actual behavior (SQ6)

SQ5: Awareness of creating a strong password * SQ6: Follow instructions when creating the password Cross tabulation							
		SQ6: Follow instructions when creating the password					Total
		Most likely	Likely	Neutral	Unlikely	Most unlikely	
SQ5: Awareness of creating a strong password	Extremely aware	125	55	10	6	1	197
	Moderately aware	36	82	13	4	1	136
	Somewhat aware	12	38	20	7	4	81
	Slightly aware	4	10	12	3	0	29
	Not at all aware	3	2	5	7	4	21
Total		180	187	60	27	10	464

Table 4.72 Chi-square result for actual awareness (SQ5) * actual behavior (SQ6)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	191.587[a]	16	.000
Likelihood Ratio	159.019	16	.000
Linear-by-Linear Association	110.789	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between cyber awareness (SQ5) and cyber behavior (SQ6) based on the above results. Therefore,

H_8 – User's cyber awareness has an impact on the user's cyber behavior

User's cyber awareness (SQ7) * user's cyber behavior (SQ8)

H_7 – User's cyber awareness has no impact on the user's cyber behavior

H_8 – User's cyber awareness has an impact on the user's cyber behavior

Table 4.73 Number of respondents answered to SQ7 and SQ8

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ7: Awareness of personal information disclosure in profile * SQ8: Currently view of email/telephone number in the profile	464	100.0%	0	0.0%	464	100.0%

Table 4.74 Cross-tabulation actual awareness (SQ7) * actual behavior (SQ8)

SQ7: Awareness of personal information disclosure in profile * SQ8: Currently view of email/telephone number in the profile Cross tabulation										
		SQ8: Currently view of email/telephone number in the profile								Total
		Public	Friends	Close friends	Acquaintances	Friends except acquaintances	Only me	Do not know	The email/telephone number/address is/are not entered in my profile	
SQ7: Awareness of personal information disclosure in profile	Extremely aware	13	78	14	0	1	139	0	13	258
	Moderately aware	4	49	11	0	0	34	5	5	108
	Somewhat aware	6	28	7	1	2	14	8	2	68
	Slightly aware	1	8	0	0	0	6	5	0	20
	Not at all aware	2	4	0	0	0	3	1	0	10
Total		26	167	32	1	3	196	19	20	464

Table 4.75 Chi-square result for actual awareness (SQ7) * actual behavior (SQ8)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	94.079[a]	28	.000
Likelihood Ratio	88.746	28	.000
Linear-by-Linear Association	6.235	1	.013
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between cyber awareness (SQ7) and cyber behavior (SQ8) based on the above results. So,

H_8 – User's cyber awareness has an impact on the user's cyber behavior

User's cyber awareness (SQ9) * user's cyber behavior (SQ10)

H_9 – User's cyber awareness has no impact on the user's cyber behavior

H_{10} – User's cyber awareness has an impact on the user's cyber behavior

Table 4.76 Number of respondents answered to SQ9 and SQ10

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ9: Awareness of two-factor authentication * S10: Use of two-factor authentication	464	100.0%	0	0.0%	464	100.0%

Table 4.77 Cross-tabulation actual awareness (SQ9) * actual behavior (SQ10)

SQ9: Awareness of two-factor authentication * S10: Use of two-factor authentication Cross tabulation				
		S10: Use of two-factor authentication		
		Yes	No	Total
SQ9: Awareness of two-factor authentication	Extremely aware	125	63	188
	Moderately aware	46	52	98
	Somewhat aware	14	45	59
	Slightly aware	2	41	43
	Not at all aware	3	73	76
Total		190	274	464

Table 4.78 Chi-square result for actual awareness (SQ9) * actual behavior (SQ10)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	125.866[a]	4	.000
Likelihood Ratio	146.565	4	.000
Linear-by-Linear Association	121.046	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between cyber awareness (SQ9) and cyber behavior (SQ10) based on the above results. Hence,

H_8 – User's cyber awareness has an impact on the user's cyber behavior

User's cyber awareness (SQ11) * user's cyber behavior (SQ12)

H_9 – User's cyber awareness has no impact on the user's cyber behavior

H_{10} – User's cyber awareness has an impact on the user's cyber behavior

Table 4.79 Number of respondents answered to SQ11 and SQ12

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ11: Awareness of setting up who can send friend requests * SQ12: Use of setting up who can send friend requests feature	464	100.0%	0	0.0%	464	100.0%

Table 4.80 Cross-tabulation actual awareness (SQ11) * actual behavior (SQ12)

SQ11: Awareness of setting up who can send friend requests * SQ12: Use of setting up who can send friend requests feature Cross tabulation				
Count				
		SQ12: Use of setting up who can send friend requests feature		
		Yes	No	Total
SQ11: Awareness of setting up who can send friend requests	Extremely aware	154	47	201
	Moderately aware	55	60	115
	Somewhat aware	18	51	69
	Slightly aware	6	23	29
	Not at all aware	6	44	50
Total		239	225	464

Table 4.81 Chi-square result for actual awareness (SQ11) * actual behavior (SQ12)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	111.485[a]	4	.000
Likelihood Ratio	119.510	4	.000
Linear-by-Linear Association	102.198	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between cyber awareness (SQ11) and cyber behavior (SQ12) based on the above results. Therefore,

H_8 – User's cyber awareness has an impact on the user's cyber behavior

User's cyber awareness (SQ19) * user's cyber behavior (SQ20)

H_9 – User's cyber awareness has no impact on the user's cyber behavior

H_{10} – User's cyber awareness has an impact on the user's cyber behavior

Table 4.82 Cross-tabulation actual awareness (SQ19) * actual behavior (SQ20)

		S20: Current view photos, videos and posts					
		Public	Friends	Close friends	Acquaintances	Friends except acquaintances	Only me
S19: Consideration of security before sharing photos, videos and posts	Most likely	20	166	166	2	6	10
	Likely	36	133	133	0	0	2
	Neutral	9	48	48	3	1	1
	Unlikely	7	23	23	1	1	0
	Most unlikely	5	9	9	0	0	0

Table 4.83 Chi-square result for actual awareness (SQ19) * actual behavior (SQ20)

Pearson Chi-Square Tests		
		$InfoDisclosure
S19: Consideration of security before sharing photos, videos and posts	Chi-square	44.903
	df	24
	Sig.	.006*,b,c

p=0.006

p<0.05

There is a relationship between cyber awareness (SQ19) and cyber behavior (SQ20) based on the above results. So,

H_8 – User's cyber awareness has an impact on the user's cyber behavior

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ4)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.84 Number of respondents answered to SQ4

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ22: Current believed behavior level of the user * SQ4: Time spent on Facebook	464	100.0%	0	0.0%	464	100.0%

Table 4.85 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ4)

SQ22: Current believed behavior level of the user * SQ4: Time spent on Facebook Cross tabulation							
		SQ4: Time spent on Facebook					Total
		0 - 3 hours	4 - 6 hours	7 - 9 hours	10 – 12 hours	12+ hours	
SQ22: Current believed behavior level of the user	Strongly agree	29	17	10	7	6	69
	Agree	87	62	24	22	17	212
	Neither agree or disagree	50	30	21	13	14	128
	disagree	28	9	8	1	2	48
	Strongly disagree	4	1	1	0	1	7
Total		198	119	64	43	40	464

Table 4.86 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ4)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	14.125[a]	16	.589
Likelihood Ratio	15.976	16	.455
Linear-by-Linear Association	.984	1	.321
N of Valid Cases	464		

p=0.589

p>0.05

There is no relationship between current believed behavior (SQ22) and actual behavior (SQ4) based on the above results. Hence,

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ6)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.87 Number of respondents answered to SQ6

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ22: Current believed behavior level of the user * SQ6: Follow instructions when creating the password	464	100.0%	0	0.0%	464	100.0%

Table 4.88 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ6)

SQ22: Current believed behavior level of the user * SQ6: Follow instructions when creating the password Cross tabulation							
		SQ6: Follow instructions when creating the password					Total
		Most likely	Likely	Neutral	Unlikely	Most unlikely	
SQ22: Current believed behavior level of the user	Strongly agree	44	18	4	3	0	69
	Agree	93	88	18	8	5	212
	Neither agree or disagree	31	57	29	8	3	128
	disagree	11	21	7	8	1	48
	Strongly disagree	1	3	2	0	1	7
Total		180	187	60	27	10	464

Table 4.89 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ6)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	62.972[a]	16	.000
Likelihood Ratio	58.789	16	.000
Linear-by-Linear Association	35.047	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between current believed behavior (SQ22) and actual behavior (SQ6) based on the above results. Therefore,

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ8)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.90 Number of respondents answered to SQ8

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ22: Current believed behavior level of the user * SQ8: Currently view of email/telephone number in the profile	464	100.0%	0	0.0%	464	100.0%

Table 4.91 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ8)

SQ22: Current believed behavior level of the user * SQ8: Currently view of email/telephone number in the profile Cross tabulation										
		SQ8: Currently view of email/telephone number in the profile								Total
		Public	Friends	Close friends	Acquaintances	Friends except acquaintances	Only me	Do not know	The email/telephone number/ address is/are not entered in my profile	
SQ22: Current believed behavior level of the user	Strongly agree	2	15	9	0	0	38	1	4	69
	Agree	10	70	11	0	1	105	5	10	212
	Neither agree or disagree	11	55	8	1	2	39	7	5	128
	disagree	3	24	4	0	0	10	6	1	48
	Strongly disagree	0	3	0	0	0	4	0	0	7
Total		26	167	32	1	3	196	19	20	464

Table 4.92 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ8)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	51.458[a]	28	.004
Likelihood Ratio	51.693	28	.004
Linear-by-Linear Association	11.571	1	.001
N of Valid Cases	464		

p=0.004

p<0.05

There is a relationship between current believed behavior (SQ22) and actual behavior (SQ8) based on the above results. So,

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ10)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.93 Number of respondents answered to SQ10

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ22: Current believed behavior level of the user * S10: Use of two-factor authentication	464	100.0%	0	0.0%	464	100.0%

Table 4.94 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ10)

SQ22: Current believed behavior level of the user * S10: Use of two-factor authentication Cross tabulation				
		S10: Use of two-factor authentication		
		Yes	No	Total
SQ22: Current believed behavior level of the user	Strongly agree	41	28	69
	Agree	104	108	212
	Neither agree or disagree	34	94	128
	disagree	9	39	48
	Strongly disagree	2	5	7
Total		190	274	464

Table 4.95 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ10)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	36.681[a]	4	.000
Likelihood Ratio	38.049	4	.000
Linear-by-Linear Association	32.484	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between current believed behavior (SQ22) and actual behavior (SQ10) based on the above results. So,

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ12)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.96 Number of respondents answered to SQ12

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ22: Current believed behavior level of the user * SQ12: Use of setting up who can send friend requests feature	464	100.0%	0	0.0%	464	100.0%

Table 4.97 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ12)

SQ22: Current believed behavior level of the user * SQ12: Use of setting up who can send friend requests feature Cross tabulation				
		SQ12: Use of setting up who can send friend requests feature		
		Yes	No	Total
SQ22: Current believed behavior level of the user	Strongly agree	45	24	69
	Agree	125	87	212
	Neither agree or disagree	54	74	128
	disagree	13	35	48
	Strongly disagree	2	5	7
Total		239	225	464

Table 4.98 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ12)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	27.299[a]	4	.000
Likelihood Ratio	27.856	4	.000
Linear-by-Linear Association	25.569	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between current believed behavior (SQ22) and actual behavior (SQ12) based on the above results. Hence,

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ13)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.99 Number of respondents answered to SQ13

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ22: Current believed behavior level of the user * SQ13: Check and update the privacy and security settings	464	100.0%	0	0.0%	464	100.0%

Table 4.100 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ13)

SQ22: Current believed behavior level of the user * SQ13: Check and update the privacy and security settings Cross tabulation							
		SQ13: Check and update the privacy and security settings					Total
		Once a week	Once a month	Once in a quarter	Once a year	Never	
SQ22: Current believed behavior level of the user	Strongly agree	9	17	17	14	12	69
	Agree	12	49	59	48	44	212
	Neither agree or disagree	1	21	34	34	38	128
	disagree	1	5	4	9	29	48
	Strongly disagree	0	0	0	0	7	7
Total		23	92	114	105	130	464

Table 4.101 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ13)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	69.979[a]	16	.000
Likelihood Ratio	68.092	16	.000
Linear-by-Linear Association	44.026	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between current believed behavior (SQ22) and actual behavior (SQ13) based on the above results. Therefore,

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ14)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.102 Number of respondents answered to SQ14

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ22: Current believed behavior level of the user * SQ14: Accept friend requests	464	100.0%	0	0.0%	464	100.0%

Table 4.103 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ14)

SQ22: Current believed behavior level of the user * SQ14: Accept friend requests Cross tabulation						
		SQ14: Accept friend requests				Total
		Always	Sometimes	Rarely	Never	
SQ22: Current believed behavior level of the user	Strongly agree	0	12	17	40	69
	Agree	2	47	47	116	212
	Neither agree or disagree	2	19	48	59	128
	disagree	2	8	14	24	48
	Strongly disagree	0	1	2	4	7
Total		6	87	128	243	464

Table 4.104 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ14)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	15.697[a]	12	.206
Likelihood Ratio	15.302	12	.225
Linear-by-Linear Association	.721	1	.396
N of Valid Cases	464		

p=0.206

p>0.05

There is no relationship between current believed behavior (SQ22) and actual behavior (SQ14) based on the above results. So,

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ15)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.105 Number of respondents answered to SQ15

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ22: Current believed behavior level of the user * SQ15: Send friend requests	464	100.0%	0	0.0%	464	100.0%

Table 4.106 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ15)

SQ22: Current believed behavior level of the user * SQ15: Send friend requests Cross tabulation						
		SQ15: Send friend requests				Total
		Always	Sometimes	Rarely	Never	
SQ22: Current believed behavior level of the user	Strongly agree	1	9	13	46	69
	Agree	1	43	37	131	212
	Neither agree or disagree	2	13	30	83	128
	disagree	1	6	8	33	48
	Strongly disagree	0	1	1	5	7
Total		5	72	89	298	464

Table 4.107 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ15)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	9.916[a]	12	.623
Likelihood Ratio	10.080	12	.609
Linear-by-Linear Association	.509	1	.476
N of Valid Cases	464		

p=0.623

p>0.05

There is no relationship between current believed behavior (SQ22) and actual behavior (SQ15) based on the above results. Hence,

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ16)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.108 Number of respondents answered to SQ16

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ22: Current believed behavior level of the user * SQ16: Clicking unknown links	464	100.0%	0	0.0%	464	100.0%

Table 4.109 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ16)

SQ22: Current believed behavior level of the user * SQ16: Clicking unknown links Cross tabulation							
		SQ16: Clicking unknown links					Total
		Most likely	Likely	Neutral	Unlikely	Most unlikely	
SQ22: Current believed behavior level of the user	Strongly agree	2	6	10	10	41	69
	Agree	8	25	35	61	83	212
	Neither agree or disagree	3	8	25	52	40	128
	disagree	2	6	9	18	13	48
	Strongly disagree	0	1	3	2	1	7
Total		15	46	82	143	178	464

Table 4.110 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ16)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	30.589[a]	16	.015
Likelihood Ratio	30.859	16	.014
Linear-by-Linear Association	4.703	1	.030
N of Valid Cases	464		

p=0.015

p<0.05

There is a relationship between current believed behavior (SQ22) and actual behavior (SQ16) based on the above results. Therefore,

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ17)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.111 Number of respondents answered to SQ17

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ22: Current believed behavior level of the user * SQ17: Password change frequency	464	100.0%	0	0.0%	464	100.0%

Table 4.112 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ17)

SQ22: Current believed behavior level of the user * SQ17: Password change frequency Cross tabulation							
		SQ17: Password change frequency					Total
		Once a month	Once in a quarter	Once in six months	Once a year	Never	
SQ22: Current believed behavior level of the user	Strongly agree	2	13	14	17	23	69
	Agree	14	22	33	67	76	212
	Neither agree or disagree	3	10	13	44	58	128
	disagree	0	0	4	6	38	48
	Strongly disagree	0	0	0	0	7	7
Total		19	45	64	134	202	464

Table 4.113 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ17)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	56.925[a]	16	.000
Likelihood Ratio	63.258	16	.000
Linear-by-Linear Association	33.649	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between current believed behavior (SQ22) and actual behavior (SQ17) based on the above results. So,

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ18)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.114 Number of respondents answered to SQ18

Case Processing Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
SQ22: Current believed behavior level of the user * SQ18: Logging out after use	464	100.0%	0	0.0%	464	100.0%

Table 4.115 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ18)

SQ22: Current believed behavior level of the user * SQ18: Logging out after use Cross tabulation							
		SQ18: Logging out after use					Total
		Most likely	Likely	Neutral	Unlikely	Most unlikely	
SQ22: Current believed behavior level of the user	Strongly agree	40	10	5	7	7	69
	Agree	55	62	29	35	31	212
	Neither agree or disagree	36	23	30	26	13	128
	disagree	7	10	9	6	16	48
	Strongly disagree	1	1	1	1	3	7
Total		139	106	74	75	70	464

Table 4.116 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ18)

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	60.701[a]	16	.000
Likelihood Ratio	54.954	16	.000
Linear-by-Linear Association	21.292	1	.000
N of Valid Cases	464		

p=0.000

p<0.05

There is a relationship between current believed behavior (SQ22) and actual behavior (SQ17) based on the above results. Hence,

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

User's current believed cyber behavior (SQ22) * user's actual cyber behavior (SQ20)

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

H10 - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform

Table 4.117 Cross-tabulation current believed behavior (SQ22) * actual behavior (SQ20)

		SQ20: Current view photos, videos and posts					
		Public	Friends	Close friends	Acquaintances	Friends except acquaintances	Only me
SQ22: Current believed behavior level of the user	Strongly agree	9	13	13	0	2	3
	Agree	32	17	17	2	3	7
	Neither agree or disagree	27	11	11	4	2	3
	disagree	8	2	2	0	1	0
	Strongly disagree	1	0	0	0	0	0

Table 4.118 Chi-square result for current believed behavior (SQ22) * actual behavior (SQ20)

Pearson Chi-Square Tests		
		$InfoDisclosure
SQ22: Current believed behavior level of the user	Chi-square	22.342
	df	24
	Sig.	.559[a,b]

p=0.559

p>0.05

There is no relationship between current believed behavior (SQ22) and actual behavior (SQ20) based on the above results. Therefore,

H9 - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform

4.2.4 Bivariate Analysis: ANOVA

As stated before, ANOVA is a technique to evaluate combinations of several independent variables or factors. This analysis aims to identify those that have a significant effect on the value of a response variable (Tavakkolkhah et al., 2018). Here the ANOVA test is used to identify the statistically significant relationship with three independent variables (age, gender, and education level) over main survey questions related to a median variable (cyber awareness). Hence, this is called three-way ANOVA. Although the respondents represent different age, gender groups, or education levels, ANOVA analysis results apply to all of them in common irrespective of age, gender, and education level differences.

Analysis of Group Age*Gender* Education level and Main Survey Questions

Table 4.119 Age * Gender* Education level-wise respondents distribution

Between-Subjects Factors			
		Value Label	N
SQ1: Age	1	18 - 24	60
	2	25 - 34	252
	3	35 - 44	99
	4	45 - 54	22
	5	55 - 64	18
	6	65+	13
SQ2: Gender	1	Male	256
	2	Female	204
	3	Other	1
	4	Prefer not to say	3
SQ3: Education level	1	Secondary education	30
	2	Certificate Level	22
	3	Diploma Level	76
	4	Bachelor's Degree/ Graduate Certificate or Diploma	193
	5	Post Graduate Certificate/Diploma	64
	6	Master Degree	77
	7	Doctoral Degree	2

SQ5

H_0 – The interaction between age, gender, and education level does not affect cyber awareness

H_1 - The interaction between age, gender, and education level does affect cyber awareness

As depicted in Table 4.120, age, gender, and education level do not individually influence SQ5 as all p>0.05. Also, the interaction between age and gender, gender and education level, and age and education level is not significant as represented by p=0.553, p=0.847, and p=0.533 respectively since all p values are above 0.05. There is no significant interaction between all three independent variables (age, gender, and education level) at once since the p=0.405 and p>0.05. Hence,

H_0 -The interaction between age, gender, and education level does not affect cyber awareness

Table 4.120 ANOVA results for Age * Gender* Education level for SQ5

Tests of Between-Subjects Effects					
Dependent Variable: SQ5: Awareness of creating a strong password					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	89.324[a]	60	1.489	1.215	.143
Intercept	150.267	1	150.267	122.680	.000
Q1	8.983	5	1.797	1.467	.200
Q2	2.017	3	.672	.549	.649
Q3	5.038	6	.840	.686	.661
Q1 * Q2	6.041	6	1.007	.822	.553
Q1 * Q3	16.660	20	.833	.680	.847
Q2 * Q3	5.047	5	1.009	.824	.533
Q1 * Q2 * Q3	17.960	14	1.283	1.047	.405
Error	493.622	403	1.225		
Total	2459.000	464			
Corrected Total	582.946	463			

SQ7

H_0 – The interaction between age, gender, and education level does not affect cyber awareness

H_1 - The interaction between age, gender, and education level does affect cyber awareness

Only age is influencing individually for SQ7 with p=0.000 and p<0.05 as illustrated in Table 4.121. The interaction between age and education level and gender and education level is significant with p=0.003 and p=0.018 respectively since both p values are less than 0.05.

However, there is no significant interaction between all three independent variables (age, gender, and education level) together since the p=0.369 and p>0.05. Thus,

H_0 -The interaction between age, gender, and education level does not affect cyber awareness

Table 4.121 ANOVA results for Age * Gender* Education level for SQ7

Tests of Between-Subjects Effects					
Dependent Variable: SQ7: Awareness of personal information disclosure in profile					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	127.648[a]	60	2.127	2.542	.000
Intercept	117.351	1	117.351	140.202	.000
Q1	24.499	5	4.900	5.854	.000
Q2	1.793	3	.598	.714	.544
Q3	5.551	6	.925	1.105	.358
Q1 * Q2	9.282	6	1.547	1.848	.089
Q1 * Q3	36.009	20	1.800	2.151	.003
Q2 * Q3	11.536	5	2.307	2.757	.018
Q1 * Q2 * Q3	12.721	14	.909	1.086	.369
Error	337.317	403	.837		
Total	1872.000	464			
Corrected Total	464.966	463			

SQ9

H_0 – The interaction between age, gender, and education level does not affect cyber awareness

H_1 - The interaction between age, gender, and education level does affect cyber awareness

As shown in Table 4.122 age (p=0.001 and p<0.05) and education level (p=0.19 and p<0.05) have an impact on SQ9. Also, age and gender have significant interaction with S9 with p=0.007 and p<0.05. The final ANOVA result shows that age, gender, and education level have a significant interaction on SQ9 with p=0.015 and p<0.05. So,

H_1 - The interaction between age, gender, and education level does affect cyber awareness

Table 4.122 ANOVA results for Age * Gender* Education level for SQ9

Tests of Between-Subjects Effects					
Dependent Variable: SQ9: Awareness of two-factor authentication					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	288.646[a]	60	4.811	2.618	.000
Intercept	261.958	1	261.958	142.547	.000
Q1	41.496	5	8.299	4.516	.001
Q2	4.285	3	1.428	.777	.507
Q3	28.188	6	4.698	2.556	.019
Q1 * Q2	32.940	6	5.490	2.987	.007
Q1 * Q3	37.496	20	1.875	1.020	.437
Q2 * Q3	20.465	5	4.093	2.227	.051
Q1 * Q2 * Q3	52.008	14	3.715	2.021	.015
Error	740.593	403	1.838		
Total	3699.000	464			
Corrected Total	1029.239	463			

SQ11

H_0 – The interaction between age, gender, and education level does not affect cyber awareness

H_1 - The interaction between age, gender, and education level does affect cyber awareness

Age and education level has an impact on S11 with a p-value less than 0.05 as displayed in Table 4.123. Also, there is a significant interaction between age, gender, and education level with p-value =0.29 and p<0.05. Therefore

H_1 - The interaction between age, gender, and education level does affect cyber awareness

Table 4.123 ANOVA results for Age * Gender* Education level for SQ11

Tests of Between-Subjects Effects					
Dependent Variable: SQ11: Awareness of setting up who can send friend requests					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	201.006[a]	60	3.350	2.169	.000
Intercept	221.346	1	221.346	143.286	.000
Q1	19.469	5	3.894	2.521	.029
Q2	2.877	3	.959	.621	.602
Q3	22.447	6	3.741	2.422	.026
Q1 * Q2	16.631	6	2.772	1.794	.099
Q1 * Q3	40.356	20	2.018	1.306	.170
Q2 * Q3	12.248	5	2.450	1.586	.163
Q1 * Q2 * Q3	40.216	14	2.873	1.860	.029
Error	622.546	403	1.545		
Total	2996.000	464			
Corrected Total	823.552	463			

SQ19

H_0 – The interaction between age, gender, and education level does not affect cyber awareness

H_1 - The interaction between age, gender, and education level does affect cyber awareness

As per results shown in Table 4.124, there is a significant interaction between age and gender with a p-value less than 0.05 when responding to SQ19. Also the interaction among age, gender, and education level is significant for SQ19 with a p-value of 0.002 and $p<0.05$. Therefore,

H_1 - The interaction between age, gender, and education level does affect cyber awareness

Table 4.124 ANOVA results for Age * Gender* Education level for SQ19

Tests of Between-Subjects Effects					
Dependent Variable: S19: Consideration of security before sharing photos, videos and posts					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	110.078[a]	60	1.835	1.933	.000
Intercept	183.226	1	183.226	193.007	.000
Q1	13.918	5	2.784	2.932	.013
Q2	1.321	3	.440	.464	.708
Q3	18.590	6	3.098	3.264	.004
Q1 * Q2	14.881	6	2.480	2.613	.017
Q1 * Q3	25.575	20	1.279	1.347	.145
Q2 * Q3	10.167	5	2.033	2.142	.060
Q1 * Q2 * Q3	33.019	14	2.358	2.484	.002
Error	382.575	403	.949		
Total	2219.000	464			
Corrected Total	492.653	463			

4.2.5 Conclusion

Data analysis is conducted on all the data collected from SSS and their results are stated in chapter 4. Descriptive analysis, chi-square analysis, and ANOVA analysis methods are used in this matter accordingly. The next step is to interpret the results revealed in data analysis and compare them with the facts found in the literature review. Chapter 5 explores this in terms of discussion of data analysis results under each aforementioned data analysis method.

5. Discussion

5.1 Introduction

This chapter is about interpreting results gained from various data analysis methods from chapter 4. In subsection 5.2 descriptive analysis results are further discussed and then chi-square data results are discussed in subsection 5.3 to identify the impact of established hypotheses. After that, a discussion on ANOVA test results is conducted in subsection 5.4. Then in subsection 5.5, the researcher will recommend practices for Facebook users based on the discussion results. Finally, the chapter is concluded in subsection 5.6.

5.2 Discussion on Descriptive Analysis

This section discovers the age, gender, and education level-wise cyber awareness level of Facebook users, the impact of cyber awareness over cyber behavior, and the impact of cyber behavior over vulnerability level of Facebook users based on the responses received for SSS. Below Table 5.1 depicts the age-wise awareness of Facebook users identified in the research

Table 5.1 Findings of descriptive analysis results related to age-wise awareness of users

Age category	Survey question	Awareness status	Percentage of responses related to awareness status	Average cyber awareness	Believed cyber awareness (At least moderate)
18-24	SQ5	At least moderately aware	71.6%	73.32%	80%
	SQ7	At least moderately aware	80%		
	SQ9	At least moderately aware	58.4%		
	SQ11	At least moderately aware	78.3%		
	SQ19	At least likely consideration	78.3%		
25-34	SQ5	At least moderately aware	75.4%	76.9%	82%
	SQ7	At least moderately aware	83.7%		
	SQ9	At least moderately aware	70.2%		
	SQ11	At least moderately aware	75%		
	SQ19	At least likely consideration	80.2%		

Age category	Survey question	Awareness status	Percentage of responses related to awareness status	Average cyber awareness	Believed cyber awareness (At least moderate)
35-44	SQ5	At least moderately aware	69.7%	70.34%	73.%
	SQ7	At least moderately aware	82.9%		
	SQ9	At least moderately aware	60.7%		
	SQ11	At least moderately aware	61.6%		
	SQ19	At least likely consideration	76.8%		
45-54	SQ5	At least moderately aware	50%	52.7%	72.7%
	SQ7	At least moderately aware	63.6%		
	SQ9	At least moderately aware	31.8%		
	SQ11	At least moderately aware	45.4%		
	SQ19	At least likely consideration	72.7%		
55-64	SQ5	At least moderately aware	66.7%	42.22%	77.8%
	SQ7	At least moderately aware	33.3%		
	SQ9	At least moderately aware	22.2%		
	SQ11	At least moderately aware	27.8%		
	SQ19	At least likely consideration	61.1%		
65+	SQ5	At least moderately aware	61.5%	43.1%	69.2%
	SQ7	At least moderately aware	38.5%		
	SQ9	At least moderately aware	23.1%		
	SQ11	At least moderately aware	30.8%		
	SQ19	At least likely consideration	61.6%		

Table 5.1 portrays that average cyber awareness is increasing from age 18- 34 and then decreasing gradually with the age range of 35- 64. Again there is a slight increase in cyber

awareness in the age 65+ group which is 0.88%. Based on the overall results shown in Table 5.1, the researcher disagrees with there was no difference in cyber hygiene knowledge among different age groups (Cain et al., 2018). The believed moderate awareness of age groups 18-24 and 25-34 is greater than their actual average awareness figures and the difference is 6.68% and 5.1% respectively. Believed moderate awareness of age group 35-44 is slightly higher than their actual average awareness level. However, there is a significant difference between believed moderate awareness and actual average awareness of respondents in the age range 45- 65+. The difference is 20%, 35.58%, and 26.1% respectively Therefore respondents from age 45 -65+ are more vulnerable to cyber threats in Facebook since they believe that they have at least moderate awareness but their actual average cyber awareness level is really low. More age-related data regarding SQ5, SQ7, SQ9, SQ11, and SQ19 are in Figures C.4, C.10, C.16, C.22, and C.46 respectively, and age-wise believed awareness data is in Figure C.49 in Appendix C. Table 5.2 illustrates the gender-wise awareness generated from responses collected via the survey.

Table 5.2 Findings of descriptive analysis results related to gender-wise awareness of users

Gender category	Survey question	Awareness status	Percentage of responses related to awareness status	Average cyber awareness	Believed cyber awareness (At least moderate)
Male	SQ5	At least moderately aware	72.6%	72.48%	82.5%
	SQ7	At least moderately aware	78.1%		
	SQ9	At least moderately aware	68.4%		
	SQ11	At least moderately aware	69.5%		
	SQ19	At least likely consideration	73.8%		
Female	SQ5	At least moderately aware	70.6%	70.26%	75%
	SQ7	At least moderately aware	79.4%		
	SQ9	At least moderately aware	52.9%		

Gender category	Survey question	Awareness status	Percentage of responses related to awareness status	Average cyber awareness	Believed cyber awareness (At least moderate)
Female	SQ11	At least moderately aware	66.1%	70.26%	75%
	SQ19	At least likely consideration	82.3%		
Other	SQ5	At least moderately aware	100%	Data is not enough since only 1 respondent in this category	Data is not enough since only 1 respondent in this category
	SQ7	At least moderately aware	100%		
	SQ9	At least moderately aware	100%		
	SQ11	At least moderately aware	100%		
	SQ19	At least likely consideration	0%		
Prefer not to say	SQ5	At least moderately aware	66.7%	Data is not enough since only 3 respondents in this category	Data is not enough since only 3 respondents in this category
	SQ7	At least moderately aware	100%		
	SQ9	At least moderately aware	66.7%		
	SQ11	At least moderately aware	66.7%		
	SQ19	At least likely consideration	100%		

According to Table 5.2, there is a slight difference between male and female average cyber awareness where males have 72.48% of average awareness while females have 70.26% of average awareness. Therefore, the researcher agrees with males have more cyber hygiene knowledge than females (Cain et al., 2018). However, collected data is not enough to comment on the average cyber awareness of others, and prefer not to say categories due to fewer respondents in those categories. Male respondents believed that they have at least a moderate level of awareness rather than 10.02% of their actual average awareness level. Female respondents believe that they have at least a moderate level of awareness rather than 4.74% from their actual average awareness level. Therefore, both genders are somewhat

vulnerable to cyber threats on Facebook based on the aforementioned difference. However, male respondents are more vulnerable than female respondents in this regard since they have the highest difference from both genders. Gender-related data regarding SQ5, SQ7, SQ9, SQ11, and SQ19 are further illustrated in Figures C.5, C.11, C.17, C.23, and C.47 respectively and gender-wise believed awareness data is in Figure C.50 in Appendix C. Table 5.3 illustrates the education level-wise cyber awareness results gained from the survey.

Table 5.3 Findings of descriptive analysis results related to education level-wise awareness of users

Education level	Survey question	Awareness status	Percentage of responses related to awareness status	Average cyber awareness	Believed cyber awareness (At least moderate)
Secondary education	SQ5	At least moderately aware	80%	78%	80%
	SQ7	At least moderately aware	83.3%		
	SQ9	At least moderately aware	66.7%		
	SQ11	At least moderately aware	76.7%		
	SQ19	At least likely consideration	83.3%		
Certificate level	SQ5	At least moderately aware	86.4%	59.98%	77.3%
	SQ7	At least moderately aware	68.2%		
	SQ9	At least moderately aware	36.3%		
	SQ11	At least moderately aware	54.5%		
	SQ19	At least likely consideration	54.5%		
Diploma level	SQ5	At least moderately aware	65.8%	64.5%	75%
	SQ7	At least moderately aware	64.5%		
	SQ9	At least moderately aware	55.3%		
	SQ11	At least moderately aware	60.6%		
	SQ19	At least likely consideration	76.3%		

Education level	Survey question	Awareness status	Percentage of responses related to awareness status	Average cyber awareness	Believed cyber awareness (At least moderate)
Bachelor's degree/ Certificate or diploma	SQ5	At least moderately aware	69.9%	74.8%	80.8%
	SQ7	At least moderately aware	82.9%		
	SQ9	At least moderately aware	68.3%		
	SQ11	At least moderately aware	71.5%		
	SQ19	At least likely consideration	81.4%		
Postgraduate certificate/ diploma	SQ5	At least moderately aware	70.4%	69.72%	81.3%
	SQ7	At least moderately aware	79.7%		
	SQ9	At least moderately aware	60.9%		
	SQ11	At least moderately aware	62.5%		
	SQ19	At least likely consideration	75.1%		
Master's degree	SQ5	At least moderately aware	76.7%	74.32%	77.9%
	SQ7	At least moderately aware	84.4%		
	SQ9	At least moderately aware	61.1%		
	SQ11	At least moderately aware	72.7%		
	SQ19	At least likely consideration	76.7%		
Doctoral degree	SQ5	At least moderately aware	50%	Data is not enough since only 2 respondents in this category	Data is not enough
	SQ7	At least moderately aware	50%		
	SQ9	At least moderately aware	0%		
	SQ11	At least moderately aware	50%		
	SQ19	At least likely consideration	50%		

As per the results shown in Table 5.3, different average cyber awareness percentage is with different education levels and there is no specific pattern can be identified with average cyber

awareness and education level. Therefore the researcher disagrees that higher education levels lead to higher information security awareness of the users (Ogutcu et al., 2016). However, the researcher is unable to comment on the average cyber awareness of doctoral degree holders since there are only two participants represent this category. All the respondents in all education levels believe that they have at least a moderate level of awareness although their actual average awareness level is lower than that. A slight difference between believed awareness and actual average awareness is identified with secondary education holders and master's degree holders. All the other respondents are comparatively vulnerable to various cyber threats in Facebook since there is a considerable difference between believed awareness and actual average awareness. Education level-wise data regarding SQ5, SQ7, SQ9, SQ11, and SQ19 are further illustrated in Figures C.6, C.12, C.18, C.24, and C.48 respectively and education level-wise believed awareness data is in Figure C.51 in Appendix C.

Ten questions in the survey are inter-related with each other in terms of user's cyber awareness and subsequent cyber behavior on Facebook. Five Facebook features/options are considered in this regard listed as below.

- Awareness of creating a strong password (SQ5) vs. follow instructions when the creation of a strong password (SQ6).
- Awareness of setting up who can view user's information feature in their profile (SQ7) vs. Current view of their email address and/or telephone number and/or address in their Facebook profile (SQ8).
- Awareness of two-factor authentication feature in Facebook (SQ9) vs. Current use of that feature (SQ10).
- Awareness of setting up who can send friend requests feature (SQ11) vs. Current use of that feature (SQ12).
- Consideration of security and privacy matters before sharing Facebook user's photos, videos, and posts in their profiles (SQ19) vs. Current view of their photos, videos, and posts they share in their profiles (SQ20).

The critical findings gained using the survey for the above combination of questions are listed in Table 5.4.

Table 5.4: Findings on users' actual cyber awareness vs. actual cyber behavior

Survey questions	Actual cyber awareness		Actual cyber behavior	
SQ5 and SQ6	At least moderately aware	71.8%	At least likely follow	79.1%
	Less than moderately aware	28.2%	Neutral or unlikely to follow	20.9%
SQ7 and SQ8	At least moderately aware	78.9%	The email/telephone number/address is/are not entered in my profile	4.3%
	Less than moderately aware	21.1%	Other options	95.7%
SQ9 and SQ10	At least moderately aware	61.6%	Yes	40.9%
	Less than moderately aware	38.4%	No	59.1%
SQ11 and SQ12	At least moderately aware	68.1%	Yes	51.5%
	Less than moderately aware	31.9%	No	48.5%
SQ19 and SQ20	At least likely consideration	77.6%	Current view photos, videos, and posts: Close Friends and Only me	10.7%
	Neutral or unlikely consideration	22.4%	Current view photos, videos, and posts: Public	14.6%

According to Table 5.4, most of the respondents are at least moderately aware of creating a strong password (71.8%) and most of them follow instructions of Facebook when creating a strong password related to their profile (79.1%) based on results shown in SQ5 and SQ6.

Based on the answers for SQ7, although 78.9% of respondents are aware of setting up who can view user's information feature in their profile, only 42.2% of respondents are using the "only me" option. Also, 4.3% of them did not enter email/telephone number/address in their profile as per SQ8. Although the respondents have selected the "only me" option, this action can provide cybersecurity to that information up to some extent as they are still not completely safe since social media sites like Facebook have stored a large amount of personal data, and thereby they have become the main target of hackers (Nyoni & Velempini, 2018). Hence if any cyber-attack happens to the Facebook platform itself and attackers can still gain access to that information. Attackers always look for vulnerabilities like users with poor best practices or more self-disclosure (Cain et al., 2018). Therefore, the researcher identifies a huge portion of respondents who are comparatively vulnerable to cyber-attacks in this regard representing 95.7% of total respondents. So that the researcher agrees with the research where it is revealed that Facebook users put high trust in the Facebook platform itself and other Facebook users. Thus they tend to share identifying information confidently on the platform (Dwyer et al., 2007; as cited by Buccafurri et al., 2015). Also, the researcher agrees that social media networks provide openness to user-profiles and the data they share in the profile. However, this openness threatened user profiles being revealed and hacked (Tang-Mui & Chan-Eang, 2017).

As per the research results shown in Table 5.4, only 8.3% of respondents in the age group 18-24, 2.8% respondents in the age group 25-34, 5.1% respondents from age group 35-44., 4.5% of respondents from age group 45-54 and 11.1% respondents from age group 55-64 did not enter their email/ telephone number/ address in their profile and majority of other respondents in all age groups reveal one or all of this information in their profiles. Therefore, the researcher agrees with the citation mentioned that most of the old and youth participants of the survey have revealed that they have shared too many personal details on social media including their phone numbers and addresses (Cain et al., 2018). A more detailed explanation is in Figure C.13 in appendix C.

61.6% of respondents are at least moderately aware of the two-factor authentication feature in Facebook but only 40.9% of them use the feature as per survey results. Also, 68.1% of survey

participants are aware of setting up who can send friend requests feature but only 51.5% of participants actually use the feature. As of the aforementioned research results, there is a significant difference between the Facebook feature awareness and usage since the usage is always low when comparing to user's awareness related to them. Hence the researcher partially agrees with feature awareness is shown to be a significant predictor of corresponding privacy behaviors in Facebook (Wisniewski et al., 2017). More illustrations on these features based on age, gender, and education levels are displayed from Figures C.16 – C.27 in Appendix C.

When it comes to consideration of security and privacy matters before sharing Facebook user's photos, videos, and posts in their profiles, 77.6% of respondents at least likely consider this. However, when it comes to actual behavior only 10.7% of them expose their photos, videos, and posts to close Friends or only to their selves. So, the researcher agrees with online privacy researches, which found users are interested in privacy protection but their actual behavior says otherwise (Barth and De Jong, 2017; Joinson et al., 2010; Tsai et al., 2006; as cited by Barth et al., 2019). However, even this portion is still vulnerable if any cyber-attack is to be taken place on the Facebook platform itself since still, attackers can gain access to their photos and videos irrespective of their current viewing condition. Also, the researcher approves that people who post information online might not think of security risks associated with it primarily. But this action can voluntarily reveal more personal information to unknown people than they expected (Nyblom, Wangen, & Gkioulos, 2020). Survey results reveal that there are no respondents who are unaware of their current view of photos, videos, and posts in their Facebook profile. Therefore, the researcher disagrees with sometimes Facebook users are unaware of the audience of their publishing posts (Johnson, Egelman, & Bellovin, 2012; as cited by Nemec Zlatolas et al., 2015). Figures C.46, C.47, and C.48 provide more illustrations on this based on age, gender, and education level in Appendix C in this regard.

The researcher partially agrees with higher awareness was connected with a lower number of reported online risk behavior (Schilder et al., 2016) based on the results displayed in Table 5.4. The $4/5^{th}$ of results illustrates that respondents still engage with risky behaviors in Facebook although they have a comparatively high level of awareness regarding that. Figure 5.1 elaborates the overview of findings based on the results received in Table 5.4.

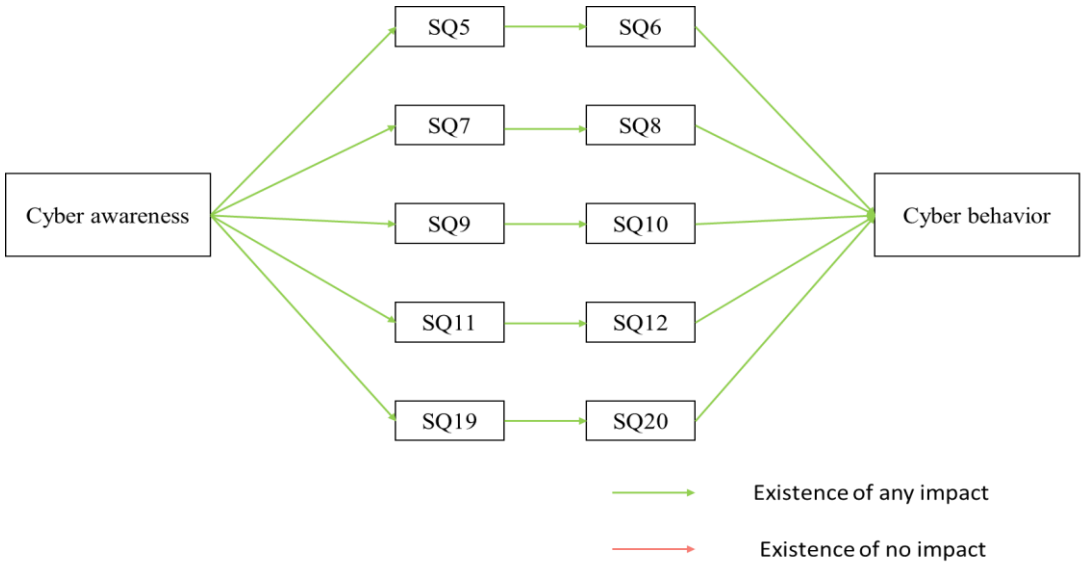


Figure 5.1: Impact of cyber awareness over cyber behavior as per discussion on descriptive analysis

Based on the discussion of descriptive analysis, the researcher discovered that there is a 100% of impact (higher or lower) from cyber awareness to cyber behavior as depicted in Figure 5.1

The descriptive analysis for the rest of the survey questions related to cyber behavior in the Facebook platform is mentioned below.

SQ4: Weekly time spent on Facebook

42.7% of respondents are currently using Facebook from 0-3 hours weekly and that is a comparatively lower amount of time. However, 17.9% of respondents use Facebook more than 10 hours per week. High-level usage of social media makes some users more vulnerable (Kaplan, & Haenlein, 2010; as cited by Atiso & Kammer, 2018). Therefore 17.9% of respondents are comparatively more vulnerable to cyber threats in Facebook as per survey results. These vulnerable respondents represent every age, gender group, and education level as depicted per the stacked bar charts C.1, C.2, and C.3 in Appendix C. Based on the survey results, the researcher could not identify any specific pattern with age and education level related to time spent on Facebook. Most of the survey participants spend less time on Facebook irrespective of their age and education levels as shown in C.1 and C.3. Therefore the researcher disagrees with social media usage decreases with age and the usage increases when income and education level increase (Hruska & Maresova, 2020).

SQ13: Check and update the privacy and security settings

Only 24.8% of respondents check and update privacy settings in their Facebook profiles on at least a monthly basis. That makes 75.2% of the respondents comparatively vulnerable to various cyber threats. Therefore the researcher agrees with most users do not check their privacy settings related to their social media accounts (Cain et al., 2018), and awareness of controlling privacy settings in social media is usually limited to the users and thereby limited in actual use as well (Pensa & Di Blasi, 2017). Age, gender, and education level-wise comprehensive illustration can be found in Figures C.28, C.29, and C.30 in Appendix C in this regard.

SQ14: Accept friend requests

52.4% of respondents never accept friend requests from unknown people on Facebook while 27.6%, 18.8%, and 1.3% of respondents accept friend requests from unknown people rarely, sometimes, and always respectively. So that 47.6% of respondents are comparatively vulnerable since spear phishing attackers send friend requests to target users to first connect with them and later make them reveal whatever information they seek or make them click malicious links (Bossetta, 2018). Figures C.31, C.32, and C.33 in Appendix C describes age, gender, and education level-wise respondent distribution comprehensively.

SQ15: Send friend requests

The percentage of survey participants who never send friend requests to unknown people on Facebook is 64.2%. This percentage is higher than those who never accept friend requests from unknown people on Facebook which is 52.4%. However 35.8% of respondents are vulnerable to cyber threats since they connect with unknown people and their photos, videos, and posts can be seen and downloaded by them unknowingly to the user. Age, gender, and education level-wise respondent distribution are portrayed in C.34, C.35, and C.36 in Appendix C accordingly.

SQ16: Clicking unknown links

69.2% of respondents are unlikely to click unknown links sent to their Facebook profile by anyone before verifying them. This will provide them security against vulnerabilities specifically from spear-phishing attacks as those attackers make users click malicious links (Bossetta, 2018). However, 30.8% of respondents are still vulnerable to cyber threats since they are likely to click links before verifying them or are neutral about this. Figures C.37,

C.38, and C.39 in Appendix C illustrate age, gender, and education level-wise information related to this matter.

S17: Password change frequency

Only 13.8% of respondents used to change their Facebook password at least once in a quarter according to survey results. The majority of respondents representing 86.2% are then vulnerable to cyber-attacks since cracking a password becomes easy with a hacker who possessed the right software tools and few personal data gained from one's social media (Eddolls, 2016). More information on age, gender, and education level-wise password changing frequencies are shown in Figures C.40, C.41, and C.42 in Appendix C.

SQ 18: Logging out after use

52.8% of respondents are likely to log out from their devices when they no longer use Facebook. But still, 47.2% of the respondents were either unlikely or neutral in this regard. This makes them vulnerable to various cyber threats if that device is lost or stolen by someone else. Figures C.43, C.44, and C.45 in Appendix C further describe age, gender, and education level-wise respondent distribution in this regard.

Figure 5.2 illustrates the presence of any vulnerability based on Facebook user behaviors as identified under the below survey questions. Here, the researcher revealed that there is a 100% impact from Facebook user's cyber behavior on the vulnerability level they face in the platform.

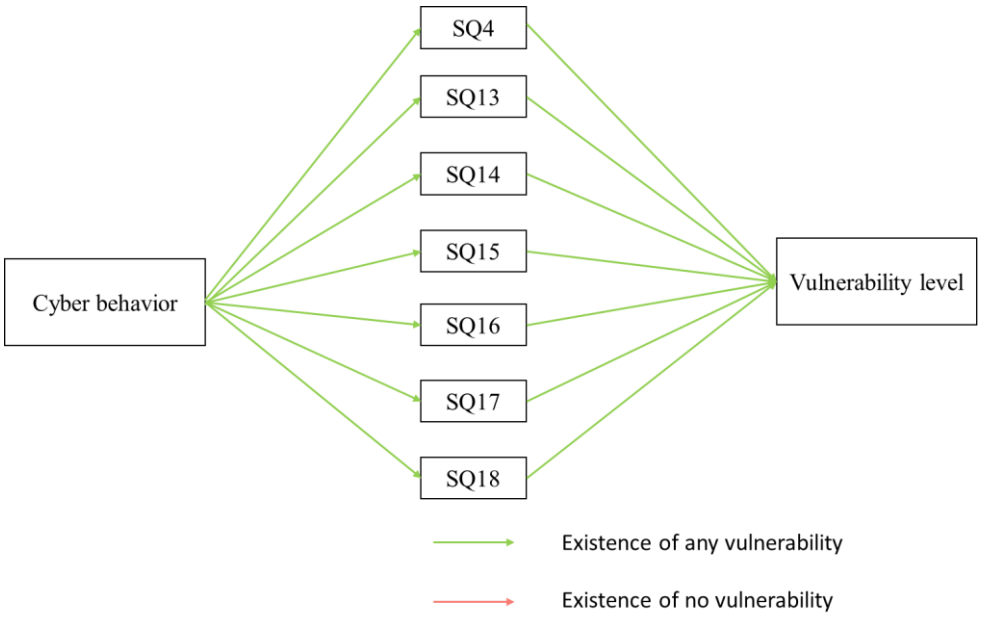


Figure 5.2: Impact of cyber behavior over vulnerability level of Facebook users

5.3 Discussion on Chi-square Analysis

The main purpose of the chi-square test is to identify the impact of variables on each other. The modified UTAUT model is used to identify the impact between independent, median, and dependent variables. Figure 5.3 depicts the modified UTAUT model used in this research.

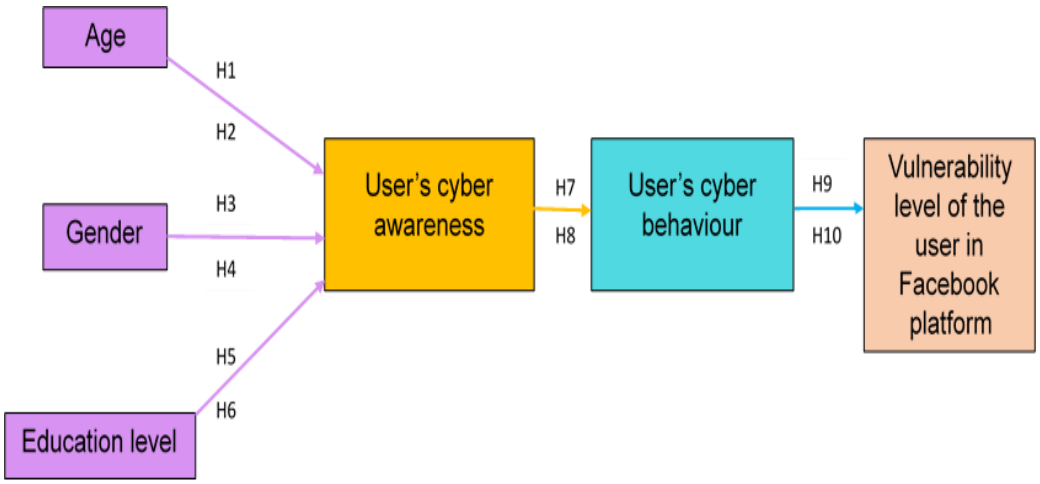


Figure 5.3: Modified UTAUT Model

Table 5.5 elaborates the impact of age over cyber awareness considering relevant survey questions, the status of hypotheses derived from chi-square analysis in subsection 4.2.3, and the weightage of impact identified over each other.

Table 5.5 Findings of chi-square test analysis results related to age

Considered variables	Considered survey questions	Status of hypothesis	Weightage of the proved impact
Age over cyber awareness	S5	**H_2: Age has an impact on the user's cyber awareness**	**80%**
	S7	**H_2: Age has an impact on the user's cyber awareness**	
	S9	**H_2: Age has an impact on the user's cyber awareness**	
	S11	**H_2: Age has an impact on the user's cyber awareness**	
	S19	**H_1: Age has no impact on the user's cyber awareness**	

Table 5.6 shows the awareness level of each age group based on the responses provided for SQ5, SQ7, SQ9, and SQ11 in the survey. Here value 1 represents the highest percentage level of awareness and the percentage decreases as the values decrease. Please note that the percentage is calculated based on the total respondents in a particular age group. A detailed illustration is in Figures in C4, C10, C16, and C.22 Appendix C.

Table 5.6 Age-wise respondent distribution and cyber awareness

Survey question	Condition	Awareness level					
		18-24	25-34	35-44	45-54	55-64	65+
SQ5 Awareness of creating a strong password	At least have a moderate level of awareness	2 71.6%	1 75.4%	3 70.7%	6 50%	4 66.7%	5 61.5%
SQ7 Awareness of personal information disclosure in profile	At least moderately aware	3 80%	1 83.7%	2 82.9%	4 63.6%	6 33.3%	5 38.5%
SQ9 Awareness of two-factor authentication	At least moderately aware	3 58.4%	1 70.2%	2 60.7%	4 31.8%	6 22.2%	5 23.1%
SQ11 Awareness of setting up who can send friend requests	At least moderately aware	1 78.3%	2 75%	3 61.6%	4 45.4%	6 27.8%	5 30.8%

As shown in Table 5.6 respondents in the age group 18-44 have more cyber awareness than respondents whose is in the age group 45-65+. That disagrees with older adults had higher Information Security Awareness (ISA) scores than young adults (McCormac et al., 2017) and surprisingly there was no difference in cyber hygiene knowledge among different age groups

(Cain et al., 2018). The above results also not supporting the following citation as well. People who have born between 1946-1962 are called “Baby Boomers” while people who are born between 1963-1978 are called “Generation X”. People born between 1979-1992 are called “Generation Y” and people born after 1992 are called “Millennials”.In the research, it is revealed that Baby Boomers are highly aware of malicious social engineering in Facebook than other younger generations (Jorgensen, 2003; Paula, & Dominic 1999; Tucker, 2006; as cited by Slonka, 2017).

Table 5.7 elaborates the impact of gender over cyber awareness using relevant survey questions, the status of hypotheses derived from chi-square analysis in subsection 4.2.3, and the weightage of impact identified over each other.

Table 5.7 Findings of chi-square test analysis results related to gender

Considered variables	Considered survey questions	Status of hypothesis	Weightage of the proved impact
Gender over cyber awareness	S5	**H_3: Gender has no impact on the user’s cyber awareness**	**20%**
	S7	**H_3: Gender has no impact on the user’s cyber awareness**	
	S9	**H_4: Gender has an impact on the user’s cyber awareness**	
	S11	**H_3: Gender has no impact on the user’s cyber awareness**	
	S19	**H_3: Gender has no impact on the user’s cyber awareness**	

Gender has a comparatively lower impact (20%) over user’s cyber awareness as depicted in Table 5.7. Table 5.8 shows the awareness level of each gender group based on the responses provided for SQ9 in the survey. A more detailed explanation can be found in Figure C17 in Appendix C.

Table 5.8 Gender-wise respondent distribution and cyber awareness

Survey question	Condition	Awareness level			
		Male	Female	Other	Prefer not to say
SQ9 Awareness of two-factor authentication	At least moderately aware	1 68.4%	2 52.9%	100%	66.7%

Elaboration in Table 5.8 shows that males have more cyber awareness than females. Based on this result the researcher agrees with males have more cyber hygiene knowledge than females (Cain et al., 2018). However, the results are shown in "Other" and "Prefer not to say" categories are not taken into account due to lower level of respondents (Other= 1, Prefer not to say= 3).

The impact of education level on cyber awareness is illustrated in Table 5.9.

Table 5.9 Findings of chi-square test analysis results related to education level

Considered variables	Considered survey questions	Status of hypothesis	Weightage of the proved impact
Education level over cyber awareness	S5	**H_5: Education level has no impact on the user's cyber awareness**	**40%**
	S7	**H_5: Education level has no impact on the user's cyber awareness**	
	S9	**H_5: Education level has no impact on the user's cyber awareness**	
	S11	**H_6: Education level has an impact on the user's cyber awareness**	
	S19	**H_6: Education level has an impact on the user's cyber awareness**	

As shown in Table 5.9 there is a 40% impact of education level over cyber awareness. Table 5.10 shows the awareness level of each education level based on the responses provided for

SQ11 and SQ19 in the survey. A more detailed explanation can be found in Figures C24 and C48 in Appendix C.

Table 5.10 Education level-wise respondent distribution and cyber awareness

Survey question	Condition	Awareness level						
		Secondary	Certificate	Diploma	Bachelor's	Postgraduate.	Master's	Doctoral
SQ11 Awareness of setting up who can send friend requests	At least moderately aware	1 76.7%	6 54.5%	5 60.6%	3 71.5%	4 62.5%	2 73%	7 50%
SQ19 Consideration of security before sharing photos, videos, and posts	At least have a likely consideration	1 83.3%	6 54.5%	4 76.3%	2 81.4%	5 75.1%	3 76.7%	7 50%

No specific pattern or trend can be identified with education level and cyber awareness from the above results. Therefore, the researcher disagrees with this citation. In the research, it is found that higher education levels lead to higher information security awareness of the users (Ogutcu et al., 2016).

Table 5.11 depicts the impact of cyber awareness on cyber behavior. Responses of SQ5 and SQ6, S7 and SQ8, SQ9 and SQ10, SQ11 and SQ12, and finally SQ19 and SQ20 are considered in this regard.

Table 5.11 Findings of chi-square test analysis results related to cyber awareness

Considered variables	Considered survey questions	Status of hypothesis	Weightage of the proved impact
Cyber awareness over cyber behavior	S5 and S6	**H_8 – User's cyber awareness has an impact on the user's cyber behavior**	**100%**
	S7 and S8	**H_8 – User's cyber awareness has an impact on the user's cyber behavior**	
	S9 and S10	**H_8 – User's cyber awareness has an impact on the user's cyber behavior**	
	S11 and S12	**H_8 – User's cyber awareness has an impact on the user's cyber behavior**	
	S19 and S20	**H_8 – User's cyber awareness has an impact on the user's cyber behavior**	

According to the results shown in Table 5.11 100% impact of cyber awareness over cyber behavior is discovered. That supports the citations, research results show that higher awareness was connected with a lower number of reported online risky behavior (Schilder et al., 2016), lack of understanding regarding appropriate cybersecurity actions can lead end users to inappropriate cyber behavior (Debatin et al., 2009; Goodhue, & Straub, 1991; Hu, Hart, & Cooke, 2006; Straub, & Welke, 1998; as cited by Cain et al., 2018), the research findings revealed that user awareness improvements lead to better security behavior (Furnell et al., 2018) and security awareness impacts user behavior when protecting against risks in information security (Herath, & Rao, 2009; Thomson, & Solms, 1998; Puhakainen, & Siponene, 2010; as cited by Torten et al., 2018).

Table 5.12 depicts the results of the relationship between actual behavior and believed behavior of users. Then the impact of actual behavior over vulnerability level is derived from that result as stated in subsection 4.2.3. After that, the weightage of the impact of cyber behavior over vulnerability level is identified and finally, the vulnerable age, gender groups, and education levels are identified accordingly.

Table 5.12 Findings of chi-square test analysis results for believed cyber awareness over actual cyber awareness

Considered survey questions	Status of hypothesis	Weightage of the proved impact	Vulnerable groups of respondents
S22 and S4	**H9** - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform	**66.7%**	All age groups, gender groups, and education levels stated under S6, S8, S10, S12, S13, S16, S17, and S18 in subsection 5.2
S22 and S6	**H10** - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform		
S22 and S8	**H10** - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform		
S22 and S10	**H10** - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform		
S22 and S12	**H10** - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform		
S22 and S13	**H10** - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform		
S22 and S14	**H9** - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform		

Considered survey questions	Status of hypothesis	Weightage of the proved impact	Vulnerable groups of respondents
S22 and S15	**H9** - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform	**66.7%**	All age groups, gender groups, and education levels stated under S6, S8, S10, S12, S13, S16, S17, and S18 as in subsection 5.2
S22 and S16	**H10** - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform		
S22 and S17	**H10** - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform		
S22 and S18	**H10** - User's cyber behavior has an impact on the vulnerability level of the user on the Facebook platform		
S22 and S20	**H9** - User's cyber behavior has no impact on the vulnerability level of the user on the Facebook platform		

As shown in Table 5.12 there is a 66.7% impact from cyber behavior over vulnerability level of Facebook users. The survey results showed no relationship between users' believed cyber behavior and how much time they spent on Facebook. Therefore no impact is identified from cyber behavior over vulnerability and hence the researcher disagrees with high-level usage of social media makes some users more vulnerable (Kaplan, & Haenlein, 2010; as cited by Atiso & Kammer, 2018). However, the researcher agrees with the following citation. In the research, it is identified that the cybersecurity behavior of the respondents potentially makes them vulnerable to cyber threats (Muniandy et al., 2017).

The modified UTAUT model with proved impact percentage of each hypothesis based on survey results is illustrated in Figure 5.2 as below.

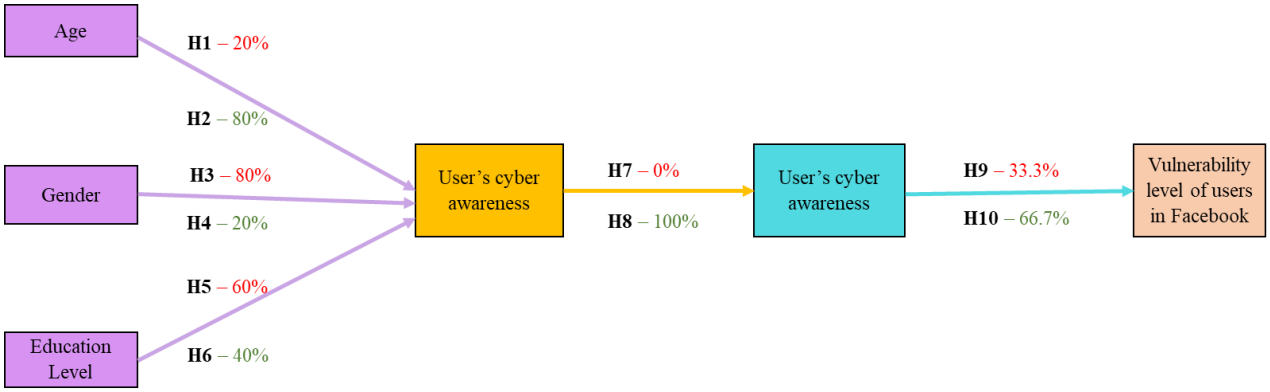


Figure 5.4: Modified UTAUT Model with proved hypotheses

Following sub-RQs are answered as below based on the chi-square analysis results.

RQ 1.1: What is the impact of the user's age on cyber awareness when using Facebook?

80% of the impact is identified from age toward cyber awareness based on research results.

RQ 1.2: What is the impact of the user's gender on cyber awareness when using Facebook?

20% of the impact is identified from gender toward cyber awareness based on research results.

RQ 1.3: What is the impact of the user's education level on cyber awareness when using Facebook?

40% of the impact is identified from education level toward cyber awareness based on research results.

RQ 1.4: What is the impact of the user's cyber awareness on the user's cyber behavior when using Facebook?

100% of the impact is identified from cyber awareness toward cyber behavior based on research results.

RQ 1.5: What is the impact of the user's cyber behavior on the user's vulnerability level when using Facebook?

66.7% of the impact is identified from cyber behavior toward vulnerability level of Facebook users based on research results.

5.4 Discussion on ANOVA Analysis

A holistic view of ANOVA data analysis results is shown in Table 5.13.

Table 5.13 Findings on overall ANOVA analysis

Survey Question	ANOVA Analysis results			
	Age * Gender	Gender * Education level	Age * Education level	Age * Gender * Education level
SQ5	No significant interaction	No significant interaction	No significant interaction	No significant interaction
SQ7	No significant interaction	There is a significant interaction	There is a significant interaction	No significant interaction
SQ9	There is a significant interaction	No significant interaction	No significant interaction	There is a significant interaction
SQ11	No significant interaction	No significant interaction	No significant interaction	There is a significant interaction
SQ19	There is a significant interaction	No significant interaction	No significant interaction	There is a significant interaction

As results shown in Table 5.13, there is less significant interaction between age and gender over cyber awareness representing only 40% of the overall significant interaction between those independent variables. The interaction between age and education and gender and education level is even lesser with only 20% of a significant interaction over cyber awareness. However, age, gender, and education level altogether have 60% of significant interaction between each other on cyber awareness revealed based on ANOVA analysis results.

5.5 Recommended Practices for Facebook Users

Base on the discussion outcomes in subsections 5.2 and 5.3, the vulnerable groups and impacts of each variable over the other are identified accordingly. When it comes to age, gender, and education level there is no 100% assurance of secured cyber behavior from all users in each group since there is at least a small portion of vulnerable respondents have identified with vulnerable behavior in the discussion of descriptive analysis subsection 5.2. The vulnerability is considered from both perspectives of individual cyber-attacks for a specific Facebook user account and cyber-attacks for the Facebook platform as a whole. There are some omissions done regarding gender-wise recommendations based on research results and they are stated with Not Applicable (NA) notation in recommendation tables. This

is due to the lower number of participants in some categories (Other=1, Prefer not to say=3). But in most cases, the researcher is not allowed to omit any age group, gender group, or education level when recommending practices for Facebook users. The researcher only considered the age, gender, and education level of the participants in New Zealand and Sri Lanka when analyzing data irrespective of the impact of other independent variables like cultural, and regulatory differences between these two countries. Therefore, the research does not cover any comparison between these two countries and thereby the recommendation is done on a common basis for both New Zealand and Sri Lankan contexts. The applicable recommended practices are noted with the letter "A" in tables accordingly. Recommendations for age-wise, gender-wise, and education level-wise categories are depicted in Table 5.14, Table 5.15, and Table 5.16 respectively.

Table 5.14 Age wise recommended practices for Facebook users

Recommended practice	18-24	25-34	35-44	45-54	55-64	65+
Follow instructions provided by Facebook when you create the password	A	A	A	A	A	A
Remove email address and/or telephone number and/or address in your Facebook profile	A	A	A	A	A	A
Use the two-factor authentication in your profile	A	A	A	A	A	A
Set up who can send you friend requests in your profile	A	A	A	A	A	A
Check and update the privacy and security settings in your profile regularly	A	A	A	A	A	A
Verify any link sent to your profile before clicking it	A	A	A	A	A	A
Change your Facebook password at least once in a quarter	A	A	A	A	A	A
Logout from your profile from any device when you no longer use Facebook in them	A	A	A	A	A	A

Table 5.15 Gender wise recommended practices for Facebook users

Recommended practice	Male	Female	Other	Prefer not to say
Follow instructions provided by Facebook when you create the password	A	A	A	A
Remove email address and/or telephone number and/or address in your Facebook profile	A	A	A	A
Use the two-factor authentication in your profile	A	A	A	A
Set up who can send you friend requests in your profile	A	A	NA	A
Check and update the privacy and security settings in your profile regularly	A	A	A	A
Verify any link sent to your profile before clicking it	A	A	NA	NA
Change your Facebook password at least once in a quarter	A	A	NA	NA
Logout from your profile from any device when you no longer use Facebook in them	A	A	A	A

Table 5.16 Education level-wise recommended practices for Facebook users

Recommended practice	Secondary	Certificate	Diploma	Bachelor's	Postgraduate.	Master's	Doctoral
Follow instructions provided by Facebook when you create the password	A	A	A	A	A	A	A

Recommended practice	Secondary	Certificate	Diploma	Bachelor's	Postgraduate.	Master's	Doctoral
Remove email address and/or telephone number and/or address in your Facebook profile	A	A	A	A	A	A	A
Use the two-factor authentication in your profile	A	A	A	A	A	A	A
Set up who can send you friend requests in your profile	A	A	A	A	A	A	A
Check and update the privacy and security settings in your profile regularly	A	A	A	A	A	A	A

Recommended practice	Secondary	Certificate	Diploma	Bachelor's	Postgraduate.	Master's	Doctoral
Verify any link sent to your profile before clicking it	A	A	A	A	A	A	A
Change your Facebook password at least once in a quarter	A	A	A	A	A	A	A
Logout from your profile from any device when you no longer use Facebook in them	A	A	A	A	A	A	A

5.6 Conclusion

All the results interpretations according to data analysis are completed in chapter 4. That marks the formal end of the research project. Next and final chapter 6 elaborates limitations of the research, future work, and conclusion remarks accordingly.

6. Conclusion

This chapter covers three subsections as it reached the end of the research report. Subsections 6.2 and 6.3 discuss limitations and future works of the research accordingly. The overall concluding remarks are in subsection 6.3.

6.1 Limitations

There are some limitations associated with the research as follows.

- Limited geographic coverage - New Zealand and Sri Lanka only
- Only a few features of Facebook are considered to collect data regarding cyber awareness in the survey
- The researcher was unable to manage to collect valid responses from 600 respondents.
- The research finding is dependent on respondents' responses and the researcher assumed that they have revealed their true nature of cyber awareness and cyber behavioral practices in the Facebook platform as it is.
- The respondents have not represented the total population equally as per age, gender groups, and education levels.
    - Eg: There are limited respondents from age 54-65, 65+, from gender other and prefer not to say categories, from education level doctoral degree
- There are some inherited limitations associated with data analysis methods.
- Time was a major barrier to the research.

6.2 Future Work

Based on the experience gained by the researcher throughout the research, it is recommended to expand this research covering more target respondents from all age and gender groups and education levels fairly and equally. Other independent variables for cyber awareness such as the field of education, the field of current employment can also take into account in future research work. Also, it is recommended to explore all other features in Facebook that influence cyber awareness and cyber behavior in the platform and identify more accurate vulnerability levels of users accordingly. Further, comprehensive research can be conducted considering the above factors, and a Facebook user awareness framework can be developed based on those findings.

6.3 Concluding Remarks

The research is designed to achieve three major objectives. They are,

- Identification of current awareness and practices of Facebook users related to their profile in terms of cybersecurity
- Identification of the vulnerability level of Facebook users based on their responses.
- Recommendation of cybersecurity practices to overcome the identified vulnerability level from the user's point of view.

All three of the above objectives are achieved at the end of the research. The main research question and the sub-research questions are answered and hypotheses are proved at the end of the research. Although this research is conducted on general cybersecurity grounds it is also significant for employers to identify their employees' cyber awareness and cyber behavioral levels since hackers are using creative and different ways to collect personal data from gullible users (Ramakrishnan & Tandon, 2018) and the impact of security breaches cannot be fully eliminated by just using security tools in computers and infrastructure. Because human error is the weakest link in the cybersecurity chain (Furnell et al., 2006; Parsons et al., 2014; Schultz, 2005; Anwar et al., 2017; Herath, & Rao, 2009; Schneie, 2004; as cited by Zwilling et al., 2020). For example, most people reuse the same obscure password for all of their login activities including their employer's network (Eddolls, 2016). Also, human beings are the central figure of cybersecurity and they should be highly equipped with security awareness to mitigate the risks they face in cyberspace (Kovacevic et al., 2020). Therefore, employees should be more careful about what they share on social media since social engineering scams are rising gradually in modern days. Those data can be used against them and their company together with other personal data that the cybercriminals collected through other consumer data breaches (Wikipedia, 2020; as cited by Sangster, 2020). Hence this research is significant for individual Facebook users as well as for all employers who seek to improve the cyber awareness and cyber behavior of their employees as well.

References

1News (Writer). (2021). Data of 533 million Facebook users leaked online. In. New Zealand: https://www.tvnz.co.nz/.

Al-Azawei, A. (2018). Predicting the adoption of social media: An integrated model and empirical study on Facebook usage *Interdisciplinary Journal of Information, Knowledge & Management, 13*, 233-238. doi:10.28945/4106

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet, 11*(3), 73. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=135682631&site=eds-live&scope=site

Ali, L. (2019). Cyber crimes - A constant threat for the business sector and its growth (A study of the online banking sector in GCC). *Journal of Developing Areas, 53*(1). Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbig&AN=edsbig.A554041623&site=eds-live&scope=site

Andrade, C. (2021). The inconvenient truth about convenience and purposive samples. *Indian Journal of Psychological Medicine, 43*(1), 86-88. doi:10.1177/0253717620977000

Atiso, K., & Kammer, J. (2018). User beware: Determining vulnerability in social media platforms for users in Ghana. *Library Philosophy & Practice*, 1-25. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=lxh&AN=133873708&site=eds-live&scope=site

Aymen, H., & Esma, A. (2020). Handling user-oriented cyber-attacks: STRIM, a user-based security training model. *Frontiers in Computer Science, 2*. doi:10.3389/fcomp.2020.00025

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics & Informatics, 41*, 55-69. doi:10.1016/j.tele.2019.03.003

Bayard, E. E. (2019). The rise of cybercrime and the need for state cybersecurity regulations. *Rutgers Computer & Technology Law Journal, 45*(2), 69-96. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=egs&AN=144292728&site=eds-live&scope=site

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users. *Information Technology & People, 28*(3), 426-441. doi:10.1108/ITP-10-2014-0232

Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal, 18*(1), 48-58. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1246231&site=eds-live&scope=site

Bloomfield, J., & Fisher, M. J. (2019). Quantitative research design. *Journal of the Australasian Rehabilitation Nurses' Association (JARNA), 22*(2), 27-30. doi:10.33235/jarna.22.2.27-30

Bosse, I., Renner, G., & Wilkens, L. (2020). Social media and Internet use patterns by adolescents with complex communication needs. *Language, Speech & Hearing Services in Schools, 51*(4), 1024-1036. doi:10.1044/2020_LSHSS-19-00072

Bossetta, M. (2018). The weaponization of social media: Spear phishing and cyber attacks on democracy. *Journal of International Affairs, 71*, 97-106. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=132491875&site=eds-live&scope=site

Boyaci, S. D. B., & Atalay, N. (2016). A scale development for 21st century skills of primary school students: A validity and reliability study. *International Journal of Instruction, 9*(1), 133-148. Retrieved from

http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1086963&site=eds-live&scope=site
Buccafurri, F., Lax, G., Nicolazzo, S., & Nocera, A. (2015). Comparing Twitter and Facebook user behavior: Privacy and other aspects. *Computers in Human Behavior, 52*, 87-95. doi:10.1016/j.chb.2015.05.045
Buzzetto-More, N., Johnson, R., & Elobaid, M. (2015). Communicating and sharing in the semantic web: an examination of social media risks, consequences, and attitudinal awareness. *Interdisciplinary Journal of e-Skills and Lifelong Learning, 11*, 47. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsgao&AN=edsgcl.430169241&site=eds-live&scope=site
Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*, 36-45. doi:10.1016/j.jisa.2018.08.002
Chandraratna, S. (2021, May 10). Brainstorming among public health experts on optimizing the health sector response to the current surge in Sri Lanka. Retrieved from https://www.who.int/srilanka/news/detail/10-05-2021-brainstorming-experts-on-health-sector-response-to-the-current-surge-in-sri-lanka
Chang, L. Y. C., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security, 97*. doi:10.1016/j.cose.2020.101959
Chen, T.-Y., Tsai, M.-C., & Chen, Y.-M. (2016). A user's personality prediction approach by mining network interaction behaviors on Facebook. *Online Information Review, 40*(7), 913-937. doi:10.1108/OIR-08-2015-0267
Costanza, D. P., Blacksmith, N., & Coats, M. (2015). Convenience samples and teaching organizational research methods. *TIP: The Industrial-Organizational Psychologist, 53*(1), 137-140. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=108438593&site=eds-live&scope=site
Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches (Fifth edition.) [image]*: Sage publications.
Davies, C., & Fisher, M. (2018). Understanding research paradigms. *Journal of the Australasian Rehabilitation Nurses' Association (JARNA), 21*(3), 21-25. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo&AN=134014168&site=eds-live&scope=site
Eddolls, M. (2016). Making cybercrime prevention the highest priority. *Network Security, 2016*(8), 5-8. doi:10.1016/S1353-4858(16)30075-7
ENISA. (2018). ENISA threat landscape report 2018: 15 top cyberthreats and trends [PDF]. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers & Security, 75*, 1-9. doi:10.1016/j.cose.2018.01.016
Goertzen, M. J. (2017). Introduction to Quantitative Research and Data. *Library Technology Reports, 53*(4), 12. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsgac&AN=edsgac.A510481059&site=eds-live&scope=site
Goh, S. H., Di Gangi, P. M., Rivera, J. C., & Worrell, J. L. (2016). Graduate student perceptions of personal social media risk: A comparison study. *Issues in Information Systems, 17*(4), 109-119. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo&AN=119120441&site=eds-live&scope=site
Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. doi:10.1016/j.cose.2017.11.015

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. doi:10.1016/j.heliyon.2017.e00346

Hruska, J., & Maresova, P. (2020). Use of Social Media Platforms among Adults in the United States—Behavior on Social Media. *Societies (2075-4698), 10*(1), 27. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=142616553&site=eds-live&scope=site

Jones, G. L., Williams, K., Edmondson-Jones, M., Prevot, J., Drabwell, J., Solis, L., . . . Mahlaoui, N. (2020). The development of a new questionnaire to measure the burden of immunoglobulin treatment in patients with primary immunodeficiencies: The IgBoT-35. *Patient Preference & Adherence, 14*, 1567-1584. doi:10.2147/PPA.S234669

Juergensen, J., & Leckfor, C. (2019). Stop pushing me away: Relative level of Facebook addiction is associated with implicit approach motivation for Facebook stimuli. *Psychological Reports, 122*(6), 2012-2025. doi:10.1177/0033294118798624

Kaba, B., & Toure, B. (2014). Understanding information and communication technology behavioral intention to use: Applying the UTAUT model to social networking site adoption by young people in a least developed country. *Journal of the Association for Information Science and Technology (Print), 65*(8), 1662-1674. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsfra&AN=edsfra.28610029&site=eds-live&scope=site

Kemp, S. (2021, January 27). Digital 2021 global overview report: Facebook's monthly active users over time [PowerPoint slide]. Retrieved from https://datareportal.com/reports/digital-2021-global-overview-report

Khalilzadeh, J., Ozturk, A. B., & Bilgihan, A. (2017). Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. *Computers in Human Behavior, 70*, 460-474. doi:10.1016/j.chb.2017.01.001

Kimberley, R., & Karl van der, S. (2020). Modelling the intended use of Facebook privacy settings. *South African Journal of Information Management, 22*(1), e1-e9. doi:10.4102/sajim.v22i1.1238

Kivunja, C. (2015). Innovative methodologies for 21st century learning, teaching and assessment: A convenience sampling investigation into the use of social media technologies in higher education. *International Journal of Higher Education, 4*(2), 1-26. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1060618&site=eds-live&scope=site

Koohang, A., Paliszkiewicz, J., & Goluchowski, J. (2018). Social media privacy concerns: trusting beliefs and risk beliefs. *Industrial Management & Data Systems, 118*(6), 1209-1228. doi:10.1108/IMDS-12-2017-0558

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors related to cyber security behavior. *IEEE Access, Access, IEEE, 8*, 125140-125148. doi:10.1109/ACCESS.2020.3007867

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology & Health Care, 25*(1), 1-10. doi:10.3233/THC-161263

Leott, Y. M. (2019). Screening out: Criminal justice students' awareness of social media usage in policing. *Cogent Social Sciences, 5*(1). doi:10.1080/23311886.2019.1573570

Mallapaty, S. (2021). India's neighbours race to sequence genomes as COVID surges. doi:https://doi.org/10.1038/d41586-021-01287-2

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156. doi:10.1016/j.chb.2016.11.065

McKechnie, D., & Fisher, M. J. (2019). Considerations when choosing a statistical method for data analysis. *Journal of the Australasian Rehabilitation Nurses' Association (JARNA), 22*(3), 20-29. doi:10.33235/jarna.22.3.20-29

Melissa, L. R., Shona, K., Siw, W., Ana Patricia, A., David, M., Matthew, J. P., . . . Group, P.-S. (2021). PRISMA-S: an extension to the PRISMA statement for reporting literature searches in systematic reviews. *Systematic Reviews, 10*(1), 1-19. doi:10.1186/s13643-020-01542-z

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cyber security, 2017 (2017)*, 1-13. doi:DOI: 10.5171/2017.800299

Mvungi, B., & Iwaihara, M. (2015). Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features. *Computers in Human Behavior, 44*, 20-34. doi:10.1016/j.chb.2014.11.023

Nalaka, S., & Diunugala, H. (2020). Factors associating with social media related crime victimization: Evidence from the undergraduates at a public university in Sri Lanka. *International Journal of Cyber Criminology, 14*(1), 174-184. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo&AN=143029465&site=eds-live&scope=site

NapoleonCat. (2021). Facebook users in New Zealand. Retrieved from https://napoleoncat.com/stats/

Nemec Zlatolas, L., Welzer, T., Hericko, M., & Holbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior, 45*, 158-167. doi:10.1016/j.chb.2014.12.012

Nyblom, P., Wangen, G., & Gkioulos, V. (2020). Risk perceptions on social media use in Norway. *Future Internet, 12*(12), 211-211. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=147738607&site=eds-live&scope=site

Nyoni, P., & Velempini, M. (2018). Privacy and user awareness on facebook. *South African Journal of Science, 114*(5/6), 27-31. doi:10.17159/sajs.2018/20170103

NZHerld. (2021, May 3). Covid 19 coronavirus: World records as many cases in one week as in first five months of pandemic. Retrieved from https://www.nzherald.co.nz/world/covid-19-coronavirus-world-records-as-many-cases-in-one-week-as-in-first-five-months-of-pandemic/D7SZAKRAF2GEQMLBGQDGKHQ3SI/

Ogutcu, G., Testik, O. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93. doi:10.1016/j.cose.2015.10.002

Opara, E. U., & Hussein, M. T. (2017). Cyber security, threat intelligence: Defending the digital platform. *Journal of International Technology and Information Management, 26*(1). Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbig&AN=edsbig.A509944416&site=eds-live&scope=site

Ortiz, J., Chih, W.-H., & Tsai, F.-S. (2018). Information privacy, consumer alienation, and lurking behavior in social networking sites. *Computers in Human Behavior, 80*, 143-157. doi:10.1016/j.chb.2017.11.005

Patrascu, P. (2019). Promoting cybersecurity culture through education. *eLearning & Software for Education, 2*, 273-279. doi:10.12753/2066-026X-19-108

Pensa, R. G., & Di Blasi, G. (2017). A privacy self-assessment framework for online social networks. *Expert Systems with Applications, 86*, 18-31. doi:10.1016/j.eswa.2017.05.054

Presthus, W., & Vatne, D. M. (2019). A survey on facebook users and information privacy. *Procedia Computer Science, 164*, 39-47. doi:10.1016/j.procs.2019.12.152

Rafael, S.-O., Ferrán, C.-L., Edoardo, A., & Craig, L. (2021). How to properly use the PRISMA statement. *Systematic Reviews, 10*(1), 1-3. doi:10.1186/s13643-021-01671-z

Ramakrishnan, U. P., & Tandon, J. K. (2018). The evolving lanscape of cyber threats. *Vidwat: The Indian Journal of Management, 11*, 31-35. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=139235797&site=eds-live&scope=site

Rice, D. B., Kloda, L. A., Shrier, I., & Thombs, B. D. (2016). Reporting completeness and transparency of meta-analyses of depression screening tool accuracy: A comparison of meta-analyses published before and after the PRISMA statement. *Journal of Psychosomatic Research, 87*, 57-69. doi:10.1016/j.jpsychores.2016.06.007

Richa, N. A. (2020). The role of effective factors in UTAUT model on behavioral intention. *Business Excellence and Management, 10*(3), 5-23. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsdoj&AN=edsdoj.6a74a8d7cb3f483aa9864d33b9a301fa&site=eds-live&scope=site

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for cyber security in schools: The human factor. *Educational Planning, 27*(2), 23-39. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1252710&site=eds-live&scope=site

Rosli, M. S., Saleh, N. S., Alshammari, S. H., Ibrahim, M. M., Atan, A. S., & Atan, N. A. (2021). Improving questionnaire reliability using construct reliability for researches in educational technology. *International Journal of Interactive Mobile Technologies, 15*(4), 109-116. doi:10.3991/ijim.v15i04.20199

Rutberg, S., & Bouikidis, C. D. (2018). Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative research. *Nephrology Nursing Journal, 45*(2), 209-213. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ccm&AN=129106232&site=eds-live&scope=site

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78. doi:10.1016/j.cose.2015.05.012

Sangster, M. (2020). When it comes to cyber security, ignorance isn't bliss – it's negligence. *Network Security, 2020*(12), 8-12. doi:10.1016/S1353-4858(20)30140-9

Sayin, B., Şahin, S., Kogias, D. G., & Patrikakis, C. Z. (2019). Privacy issues in post dissemination on Facebook. *Turkish Journal of Electrical Engineering & Computer Sciences, 27*(5), 3417-3432. doi:10.3906/elk-1811-25

Schilder, J., Brusselaers, M., & Bogaerts, S. (2016). The effectiveness of an intervention to promote awareness and reduce online risk behavior in early adolescence. *Journal of Youth & Adolescence, 45*(2), 286-300. doi:10.1007/s10964-015-0401-2

Shryock, T. (2019). The growing cyber threat: Practices are increasingly coming under attack by cyber criminals. *Medical Economics, 96*(10), 22. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsgac&AN=edsgac.A590952666&site=eds-live&scope=site

Slonka, K. J. (2017). Awareness of malicious social engineering among Facebook users *Issues in Information Systems, 18*(1), 78-86. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo&AN=125260209&site=eds-live&scope=site

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems, 92*, 178-188. doi:10.1016/j.future.2018.09.063

Svoboda, J. A. N., & Lukas, L. (2019). Sources of threats and threats in cyber security. *DAAAM International Scientific Book*, 321-330. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo&AN=140062921&site=eds-live&scope=site

Szumski, O. (2018). Cybersecurity best practices among Polish students. *Procedia Computer Science, 126*, 1271-1280. doi:10.1016/j.procs.2018.08.070

Tang-Mui, J., & Chan-Eang, T. (2017). Impacts of social media (Facebook) on human communication and relationships: A view on behavioral change and social unity. *International Journal of Knowledge Content Development & Technology, 7*(4), 27-50. doi:10.5865/IJKCT.2017.7.4.027

Tankovska, H. (2021, January 28). Number of global social network users 2017-2025. Retrieved from https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Tasevski, P. (2016). IT and cyber security awareness-raising campaigns. *Information & Security, 34*(1), 7. doi:10.11610/isij.3401

Tavakkolkhah, P., Zimmer, R., & Kuffner, R. (2018). Detection of network motifs using three-way ANOVA. *PLoS ONE, 13*(8), 1-23. doi:10.1371/journal.pone.0201382

Thakur, A., & Kang, T. K. (2018). Gender and locale differences in cyber crime awareness among adolescents. *Indian Journal of Health & Wellbeing, 9*(8/9), 906-916. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=134949110&site=eds-live&scope=site

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security, 79*, 68-79. doi:10.1016/j.cose.2018.08.007

Tripathi, E., Tripathi, A., & Yadav, M. K. S. (2016). Role of information technology in cyber crime and ethical issues in cyber ethics. *International Journal of Business & Engineering Research, 10*, 1-5. Retrieved from http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=egs&AN=139360194&site=eds-live&scope=site

Ursachi, G., Horodnic, I. A., & Zait, A. (2015). How Reliable are Measurement Scales? External Factors with Indirect Influence on Reliability Estimators. *Procedia Economics and Finance, 20*, 679-686. doi:10.1016/S2212-5671(15)00123-9

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547-559. doi:10.1016/j.chb.2017.05.038

Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication, 20*(1), 83-98. doi:10.1111/jcc4.12100

Weller, K. (2016). Trying to understand social media users and usage. *Online Information Review, 40*(2), 256-264. doi:10.1108/OIR-09-2015-0299

Wilson, J. (2021, January 11). Chinese start-up leaked 400GB of scraped data exposing 200+ million Facebook, Instagram and LinkedIn users. Retrieved from https://www.safetydetectives.com/blog/socialarks-leak-report/#review-3

Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human - Computer Studies, 98*, 95-108. doi:10.1016/j.ijhcs.2016.09.006

Yau, J. C., & Reich, S. M. (2019). "It's just a lot of work": Adolescents' self-presentation norms and practices on Facebook and Instagram. *Journal of Research on Adolescence (Wiley-Blackwell), 29*(1), 196-209. doi:10.1111/jora.12376

Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems, 86*, 914-925. doi:10.1016/j.future.2016.10.007

Zikmund, W. G., Babin, B. J., Carr, J. C., & Giffin, M. (2013). *Business Research Methods, Ninth Edition.* USA: Cengage.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A Comparative Study. *Journal of Computer Information Systems*, 1-16. doi:10.1080/08874417.2020.1712269

Appendix A – Survey Questions

Screening Questions

1) Are you 18 years old or above by the time you see this survey?
2) Which country are you currently living in?
3) Are you currently using the Facebook social media platform?

Survey Questions

No	Sample Questionnaire	Answers
S1	What is your age group?	18-24 25-34 35-44 45-54 55-64 65+
S2	What is your gender?	Male Female Other Prefer not to say
S3	What is your highest completed education qualification at the moment?	Secondary education Certificate Level Diploma Level Bachelor's Degree/ Graduate Certificate or Diploma Post Graduate Certificate/Diploma Master Degree Doctoral Degree Please mention if other : _____
S4	How much time do you spend on Facebook in a week on average?	0 – 3 hours 4 – 6 hours 7 – 9 hours

		10 – 12 hours 12+ hours
S5	Are you aware that the Facebook platform provides instruction on creating a strong password?	Extremely aware Moderately aware Somewhat aware Slightly aware Not at all aware
S6	Did you follow those instructions when you create the password?	Most likely Likely Neutral Unlikely Most unlikely
S7	Are you aware that the Facebook platform provides an option to set who can view your personal information in your profile?	Extremely aware Moderately aware Somewhat aware Slightly aware Not at all aware
S8	Currently, who can view your email address and/or telephone number and/or address in your Facebook profile?	Public Friends Close friends Friends except for acquaintances Acquaintances Only me Do not know The email/telephone number/address is/are not entered in my profile
S9	Are you aware that the Facebook platform provides a two-factor authentication feature for accessing your profile?	Extremely aware Moderately aware Somewhat aware Slightly aware Not at all aware

S10	Are you currently using the two-factor authentication in your profile?	Yes No
S11	Are you aware that the Facebook platform provides an option to set who can send you friend requests?	Extremely aware Moderately aware Somewhat aware Slightly aware Not at all aware
S12	Are you currently using that option in your profile?	Yes No
S13	How often do you check and update the privacy and security settings in your profile?	Once a week Once a month Once in a quarter Once a year Never
S14	Do you accept friend requests from unknown people?	Always Sometimes Rarely Never
S15	Do you send friend requests to unknown people?	Always Sometimes Rarely Never
S16	Do you click any link sent to your profile by your friend(s) or any person before verifying it?	Most likely Likely Neutral Unlikely Most unlikely
S17	How often do you change your Facebook password?	Once a month Once in a quarter Once in six months Once a year Never

S18	Do you log out from your profile on any device when you no longer use it?	Most likely Likely Neutral Unlikely Most unlikely
S19	Do you consider the security and privacy matters before sharing your photos, videos, and posts in your profile?	Most likely Likely Neutral Unlikely Most unlikely
S20	Currently, who can view your photos, videos, and posts you share in your profile?	Public Friends Close friends Friends except for acquaintances Acquaintances Only me Do not know
S21	What level of awareness do you believe that you currently have regarding cyber threats on Facebook?	Strong level of awareness Moderate level of awareness A lower level of awareness No awareness at all
S22	Do you believe that you have taken enough precautions to safeguard your Facebook profile from cyber threats?	Strongly agree Agree Neutral Disagree Strongly disagree

Appendix B – Coding Structure Used in SPSS

Table B.1 SQ1 Coding

Age	Code
18-24	1
25-34	2
35-44	3
45-54	4
55-64	5
65+	6

Table B.2 SQ2 Coding

Gender	Code
Male	1
Female	2
Other	3
Prefer not to say	4

Table B.3 SQ3 Coding

Education Level	Code
Secondary Education	1
Certification Level	2
Diploma Level	3
Bachelor’s Degree/Graduate Certificate or Diploma	4
Post Graduate Certificate/ Diploma	5
Master’s Degree	6
Doctoral Degree	7
Please mention if other	8

Table B.4 SQ3 Coding for text input

Education Level Text Input	Code
Undergraduate Doctor of Medicine	1
OL and AL	1
After AL	1
Some College	1
Trade Certified	2
Higher National Diploma	3
BSC	4
Following MBA	4
FRACS FRCPA	4

Table B.5 SQ4 Coding

Hours Spent on Facebook	Code
0-3 hours	1
4-6 hours	2
7-9 hours	3
10-12 hours	4
12+ hours	5

Table B.6 SQ5, SQ7, SQ9, SQ11

Answer	Code
Extremely aware	1
Moderately aware	2
Somewhat aware	3
Slightly aware	4
Not at all aware	5

Table B.7 SQ6, S16, S18, S19

Answer	Code
Most likely	1
Likely	2
Neutral	3
Unlikely	4
Most unlikely	5

Table B.8 SQ8, S20

Answer	Code
Public	1
Friends	2
Close friends	3
Acquaintances	4
Friends except for acquaintances	5
Only me	6
Do not know	7
The email/telephone number is/are not entered in my profile	8

Table B.9 SQ10, SQ 12,

Answer	Code
Yes	1
No	2

Table B.10 SQ13

Answer	Code
Once a week	1
Once a month	2
Once in a quarter	3
Once a year	4
Never	5

Table B.11 SQ14, SQ15

Answer	Code
Always	1
Sometimes	2
Rarely	3
Never	4

Table B.12 SQ17

Answer	Code
Once a month	1
Once in a quarter	2
Once in six month	3
Once a year	4
Never	5

Table B.13 SQ21

Answer	Code
Strong level of awareness	1
Moderate level of awareness	2
A lower level of awareness	3
No awareness at all	4

Table B.14 SQ22

Answer	Code
Strongly agree	1
Agree	2
Neither agree or disagree	3
Disagree	4
Strongly disagree	5

Table B.15 Survey question numbers and labels

Survey question	Label in "Variable view" in SPSS
SQ1	SQ1: Age
SQ2	SQ2: Gender
SQ3	SQ3: Education level
SQ4	SQ4:Time spent on FB
SQ5	SQ5: Awareness of creating a strong password
SQ6	SQ6: Follow instructions when creating a password
SQ7	SQ7: Awareness of personal information disclosure in profile
SQ8	SQ8: Current view of email/telephone number in the profile
SQ9	SQ9: Awareness of two-factor authentication
SQ10	SQ10: Use of two-factor authentication
SQ11	SQ11: Awareness of setting up who can send friend requests
SQ12	SQ12: Use of setting up who can send friend requests feature
SQ13	SQ13: Check and update the privacy and security settings
SQ14	SQ14: Accept friend requests
SQ15	SQ15: Send friend requests
SQ16	SQ16: Clicking unknown links
SQ17	S17: Password change frequency
SQ18	SQ 18: Logging out after use
SQ19	SQ19: Consideration of security before sharing photos, videos, and posts
SQ20	S20: Current view of photos, videos, and posts
SQ21	S21: Current believed awareness level of the user
SQ22	S22: Current believed behavior level of the user

Appendix C – Descriptive Analysis with Stacked Bar Charts

As depicted in Figure C.1, the majority of the age groups from 18-24, 25-34, and 35-44 use Facebook for 0-3 hours per week. Age groups including 45-54, 55-64, and 65+ mostly use Facebook for 4-6 hours weekly representing 40.9%, 44.4%, and 69.2% respectively. 21.7% of age 18-24, 19.8% of age 25-34, and 16.2% of age 35-44 use Facebook more than 10 hours per week.

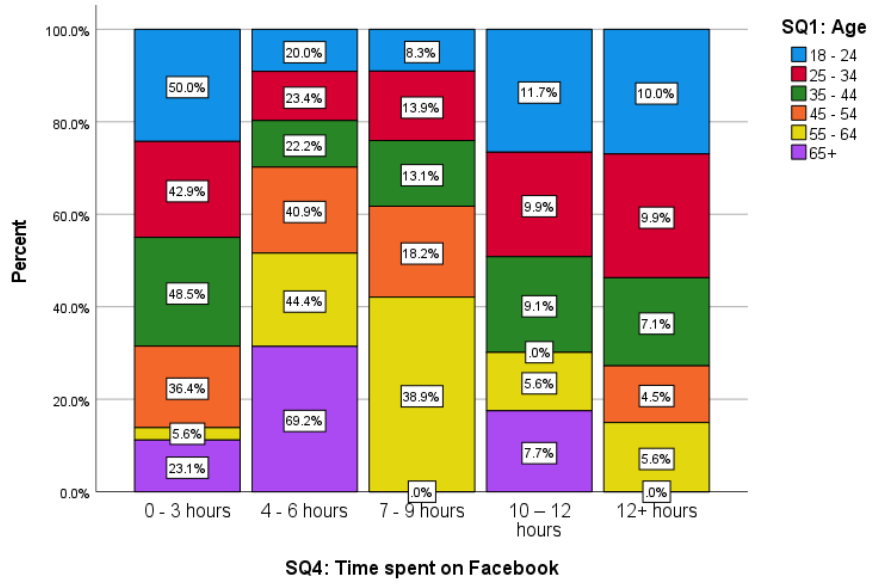


Figure C.1: Age-wise distribution related to time spent on Facebook

Figure C.2 shows that 42.6% of males, 41.7% of females, 100% of others, and 100% of prefer not to reveal their gender use Facebook for 0-3 hours weekly. 14.9% of males use Facebook more than 10 hours per week. 22.1% of females use Facebook more than 10 hours per week.

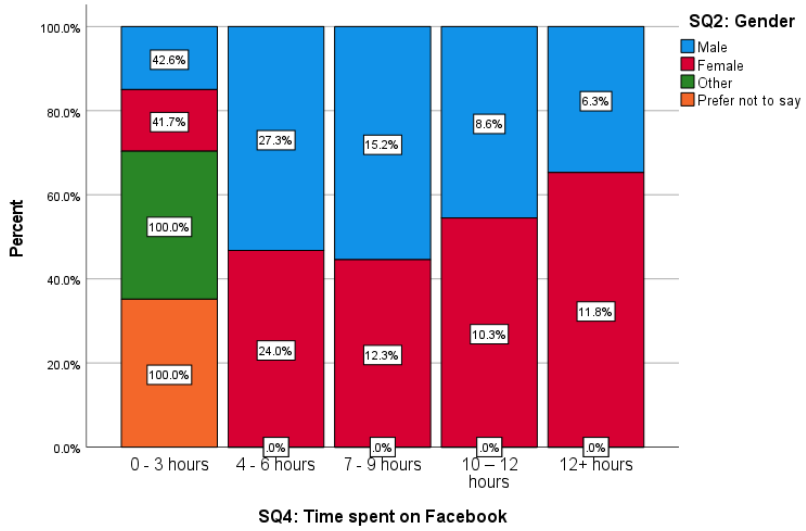


Figure C.2: Gender wise distribution related to time spent on Facebook

The majority of the education level holders use Facebook 0-3 hours weekly including secondary education -50%, certificate level 63.6%, diploma level-34.2%, bachelor's degree/graduate certificate or diploma-42.5%, postgraduate certificate/diploma- 42.2%, and master's degree 44.2%. 100% of the doctoral degree holders use Facebook for 4-6 hours weekly. 21.9% of postgraduate certificate/diploma holders use Facebook more than 10 hours per week followed by 21.1% - Diploma level holders, 20% of the secondary education holders, 19.5% of master's degree holders, and 16.1% of bachelor's degree/graduate certificate or diploma holders. These figures are further illustrated in Figure C.3.

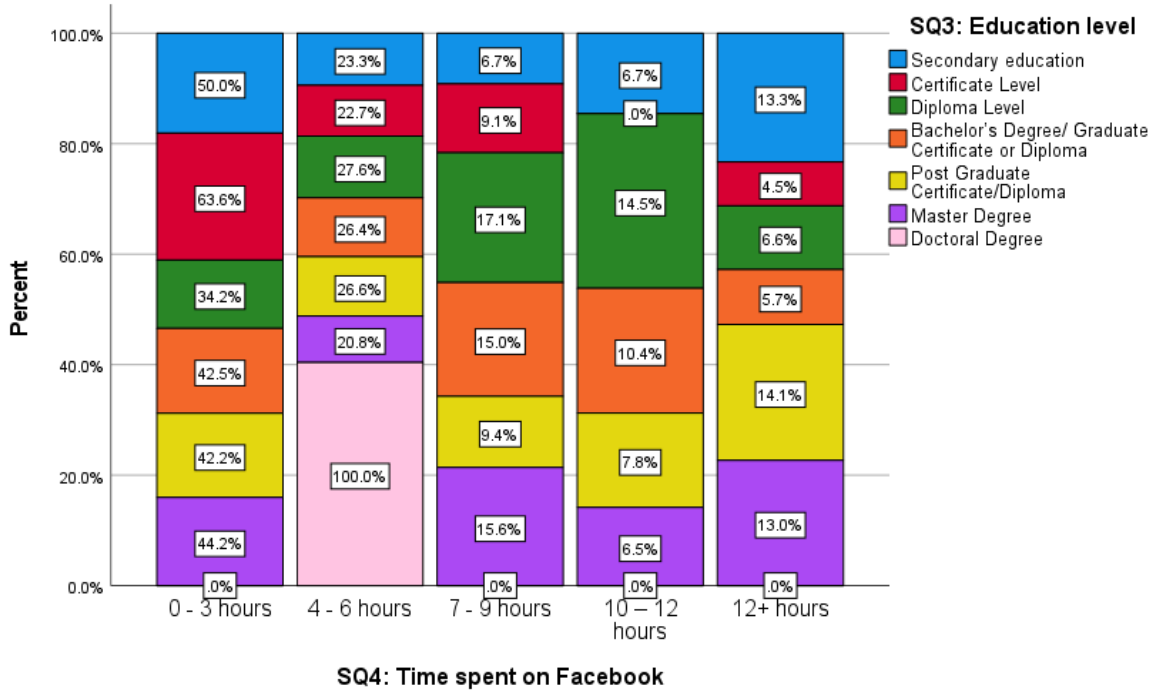


Figure C.3: Education level-wise distribution related to time spent on Facebook

The majority of respondents are extremely aware or moderately aware of creating a strong password.13.6% of the age 45-54 group are not aware of creating a strong password at all followed by 7.1% from age 35-44. The age 65+ group consists of 23.1% of people who are slightly aware of creating a strong password. Age group 45-54 also comprise 18.2% of people who are slightly aware of creating a strong password. All the illustrations are in Figure C.4.

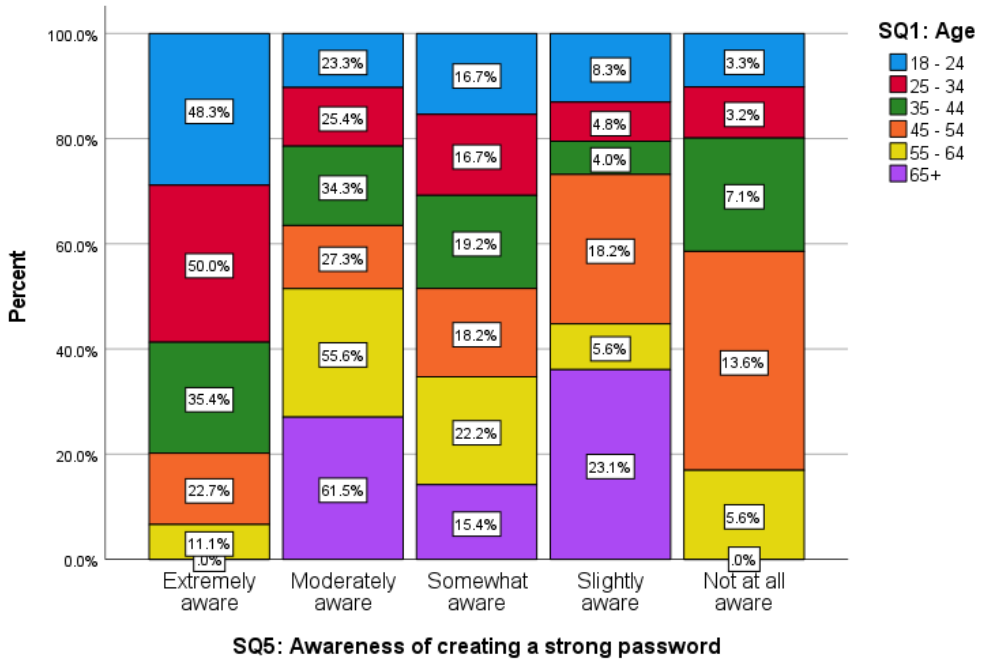


Figure C.4: Age-wise distribution related to awareness of creating a strong password

41% of males are extremely aware and 31.6% of males are moderately aware of creating a strong password. 44.1% of females are extremely aware and 26.5% of females are moderately aware of creating a strong password. Only 4.7% of males and 4.4% of females are not aware of creating a strong password at all as depicted in Figure C.5.

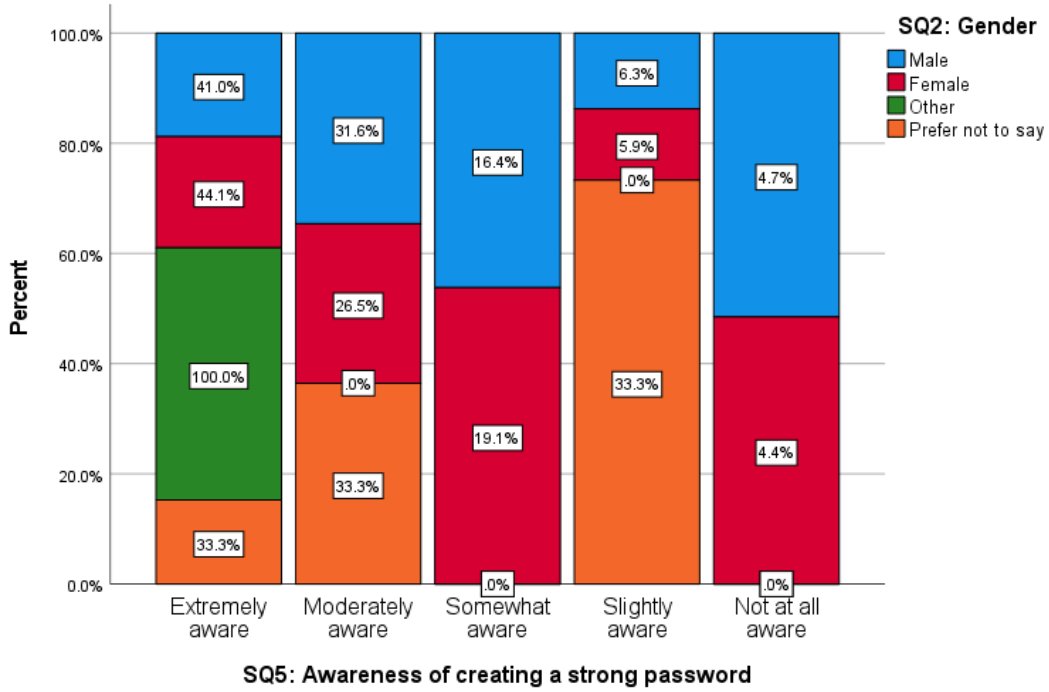


Figure C.5: Gender wise distribution related to awareness of creating a strong password

60% secondary education holders, 45.5% certificate holders, 40.8% diploma holders, 38.3% bachelor's degree/graduate certificate or diploma holders, and 43.8% postgraduate certificate/diploma holders, and 46.8% of Master's degree holders are aware of creating a strong password and those figures represent the majority of each education level as shown in Figure C.6. 50% doctoral degree holders either moderately aware or slightly aware with this regard.

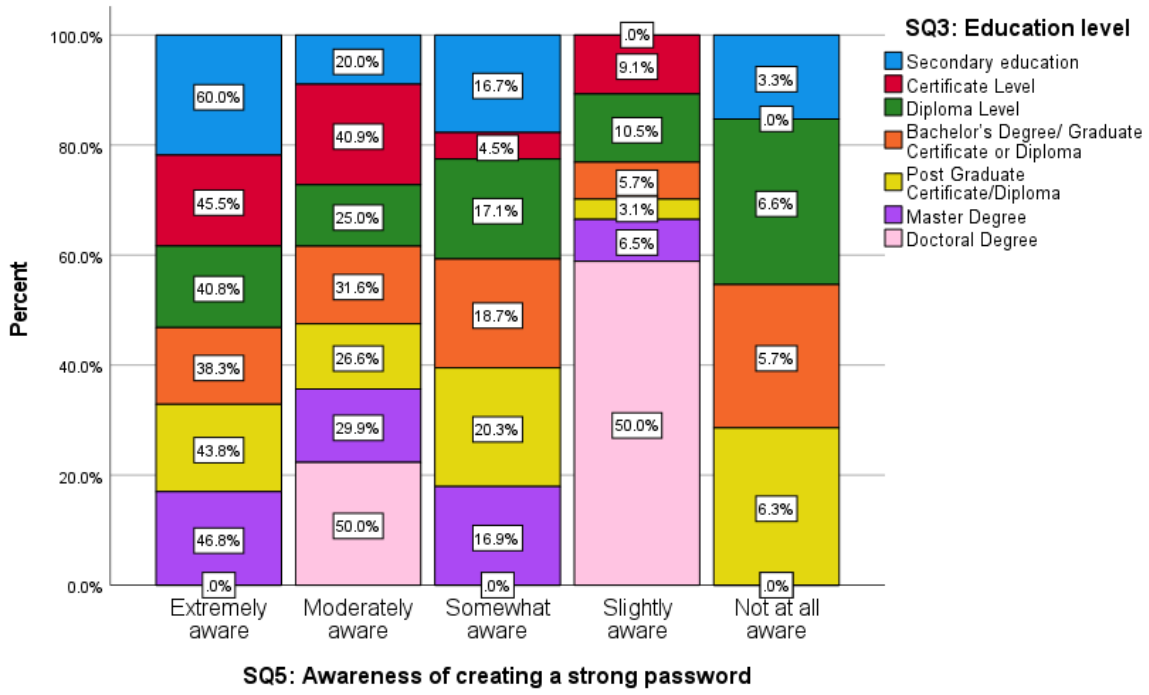


Figure C.6: Education level-wise distribution related to awareness of creating a strong password

As depicted in Figure C.7 2.8% of respondents from age 25-34 and 3% of respondents from age 35-44% are most unlikely to follow orders when creating the password. However, the majority of respondents are likely to follow the instructions provided by Facebook when creating passwords representing more than 75% positive responses from age between 18-34. The majority of respondents between the ages of 35-64 are also like to follow the instructions marking more than 70% of the total respondents. 53.8% of age 65+ respondents are also likely to follow the instructions.

Figure C.7: Age-wise distribution related to following instructions when creating a strong password

76.6% of males, 82.8% of females, and 66.7% of prefer not to say category are likely to follow instructions provided by Facebook when creating the password while the rest of the males, females and prefer not to say category are neutral or unlikely about this matter as illustrated in C.8. 100% of other category is neutral regarding in this regard.

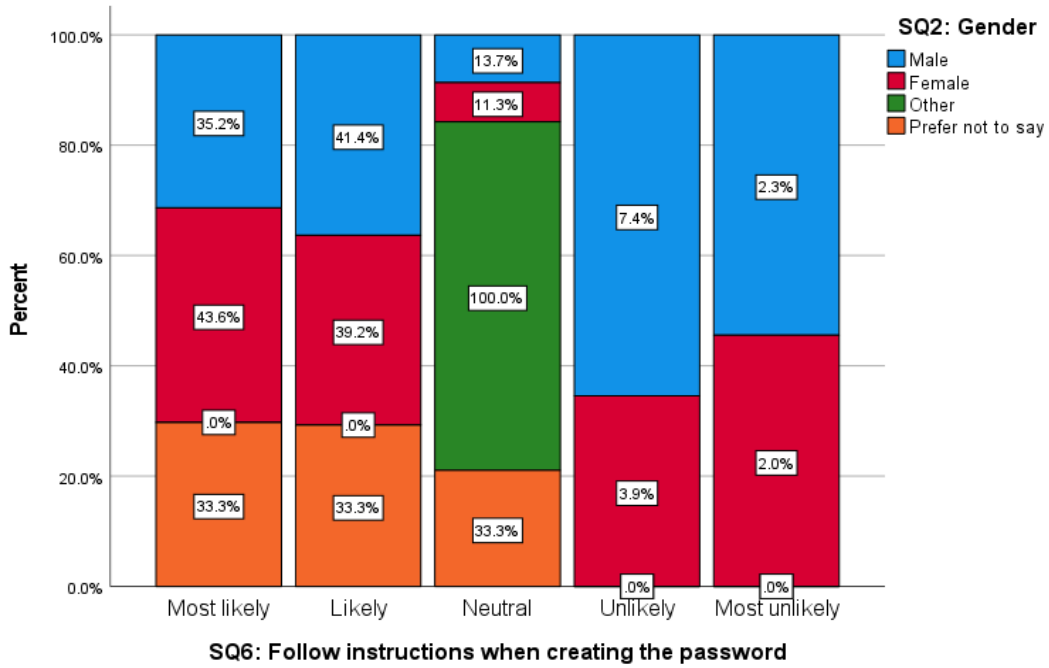


Figure C.8: Gender-wise distribution related to following instructions when creating a strong password

More than 75% of respondents from secondary, diploma, bachelor's degree/graduate certificate or diploma and master's education levels are likely to follow instructions provided by Facebook when creating the password as shown in C.9. The percentage is more than 70% when it comes to certificate level and postgraduate certificate/diploma. 50% of doctoral degree holders are either likely or neutral in this matter.

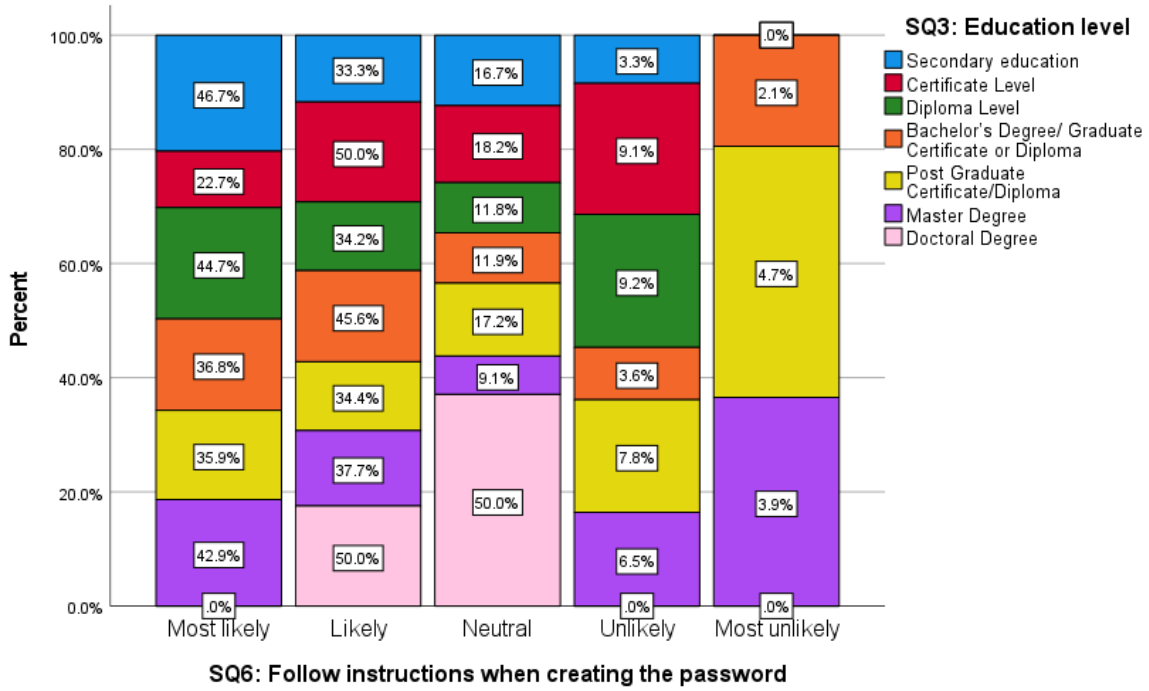


Figure C.9: Education level-wise distribution related to following instructions when creating a strong password

As shown in C.10, 80% of respondents from age 18-24, 83.7% of respondents from age 25-34, 82.9% of respondents from age 35- 44 are at least moderately aware of disclosing personal information in their Facebook profile. The figures are 63.6% of age in between 45-54, 33.3% of age in between 55-64 and 38.5 in age over 65 with the same regard. That highlight the respondents with age between 18-44 have more moderate awareness regarding personal information disclosure in the Facebook profile than respondents with age in between 45-65+.

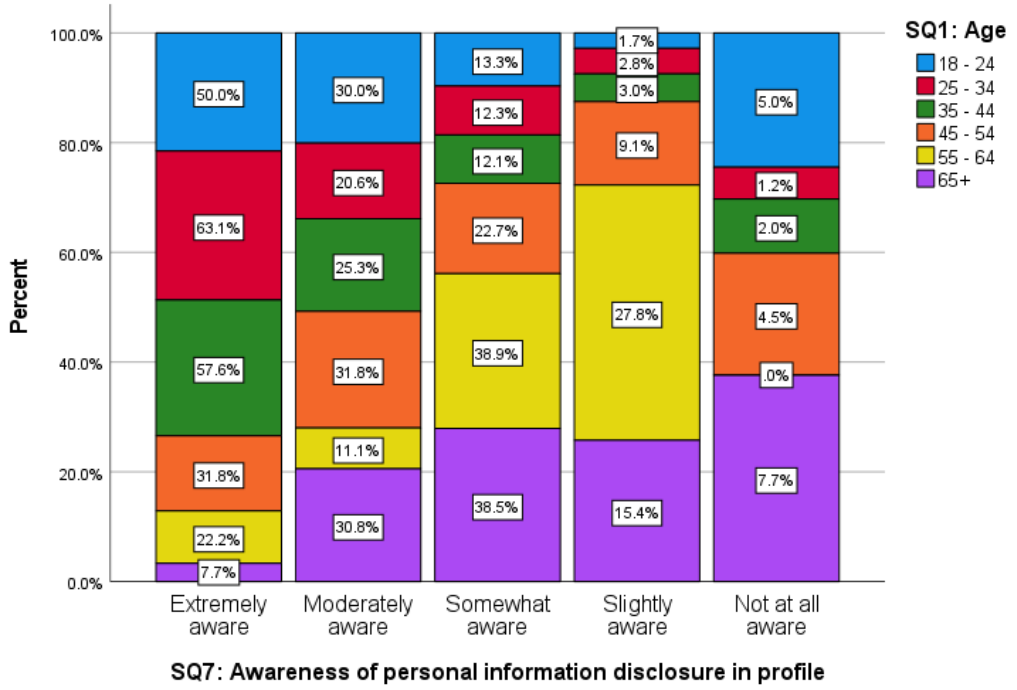


Figure C.10: Age-wise distribution related to awareness of personal information disclosure in Facebook profile

More than 75% of male and female respondents are at least moderately aware of personal information disclosure in Facebook profiles depicting almost the same percentage in Figure C.11. Other and prefer not to say categories are 100% extremely aware of with this regard.

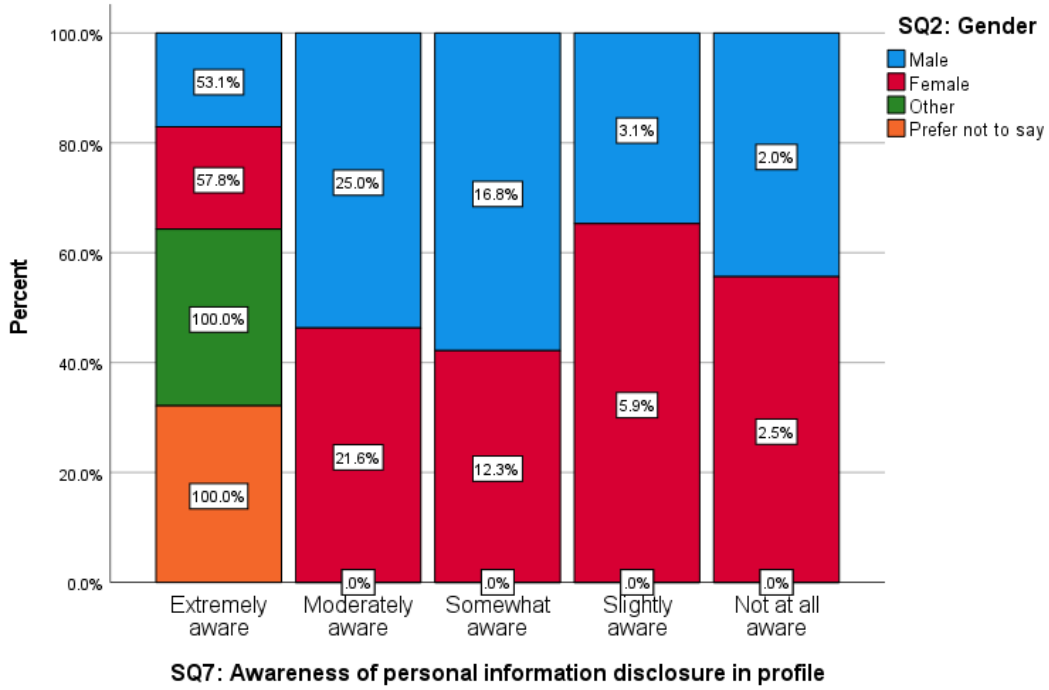


Figure C.11: Gender-wise distribution related to awareness of personal information disclosure in Facebook profile

Master's degree holders with 84.4%, secondary education holders with 83.3%, and bachelor's degree/graduate certificate or diploma holders with 82.9% represent the highest moderate awareness of personal information disclosure in Facebook profile as displayed in Figure C.12. Please note that figures in extremely aware and moderately aware are combined to generate the above figures. Postgraduate Certificate/diploma holders represent 79.7%, certificate level holders represent 68.2%, and diploma level holders represent 64.5% of moderate level awareness on disclosing personal information in Facebook profiles.

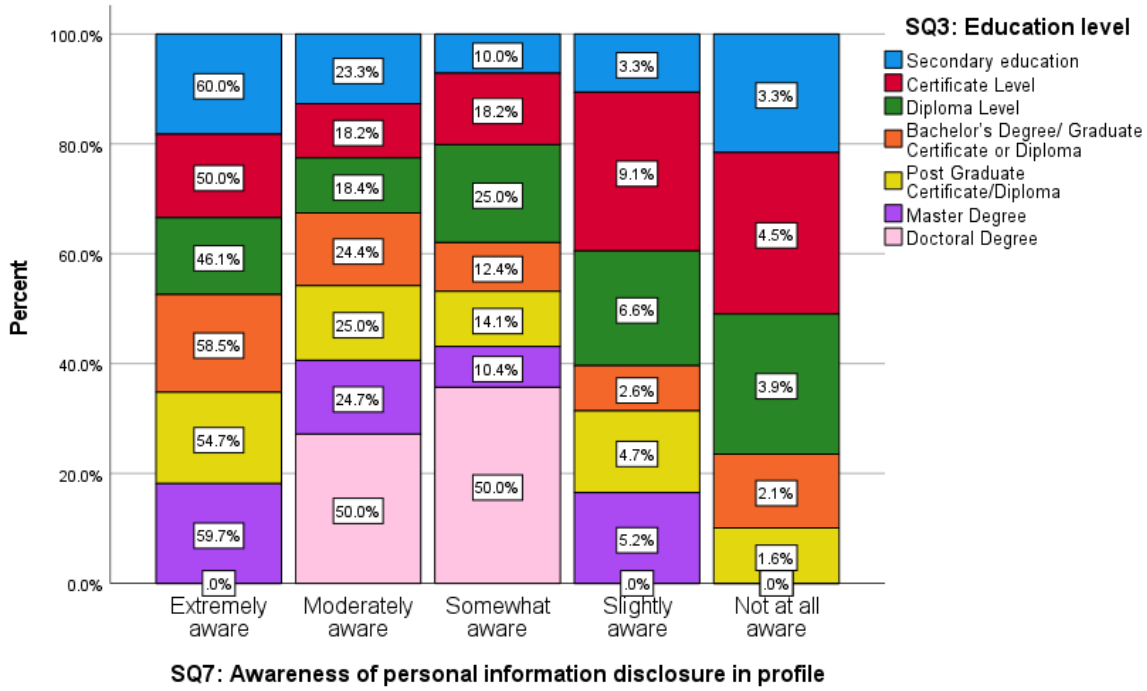


Figure C.12: Education level-wise distribution related to awareness of personal information disclosure in Facebook profile

As depicted in C.13, 41.7% of respondents from age group 18-24, 51.6% of respondents from age group 25-34, 34.3% of respondents from age group 35-44, 27.3% of respondents from age group 45-54 and 5.6% of respondents from age group 55-64 are currently viewing their email/telephone number or address only to themselves in their Facebook profile. Although that provides some protection to personal details in the profile still they are vulnerable if the Facebook platform itself is targeted to a cyber-attack and those details are still extractable by the attackers. Therefore only true non-vulnerable Facebook users in this regard are the respondents who select the option "The email/telephone number/address is/are not entered in my profile" which represents a smaller portion of total respondents in each age group.

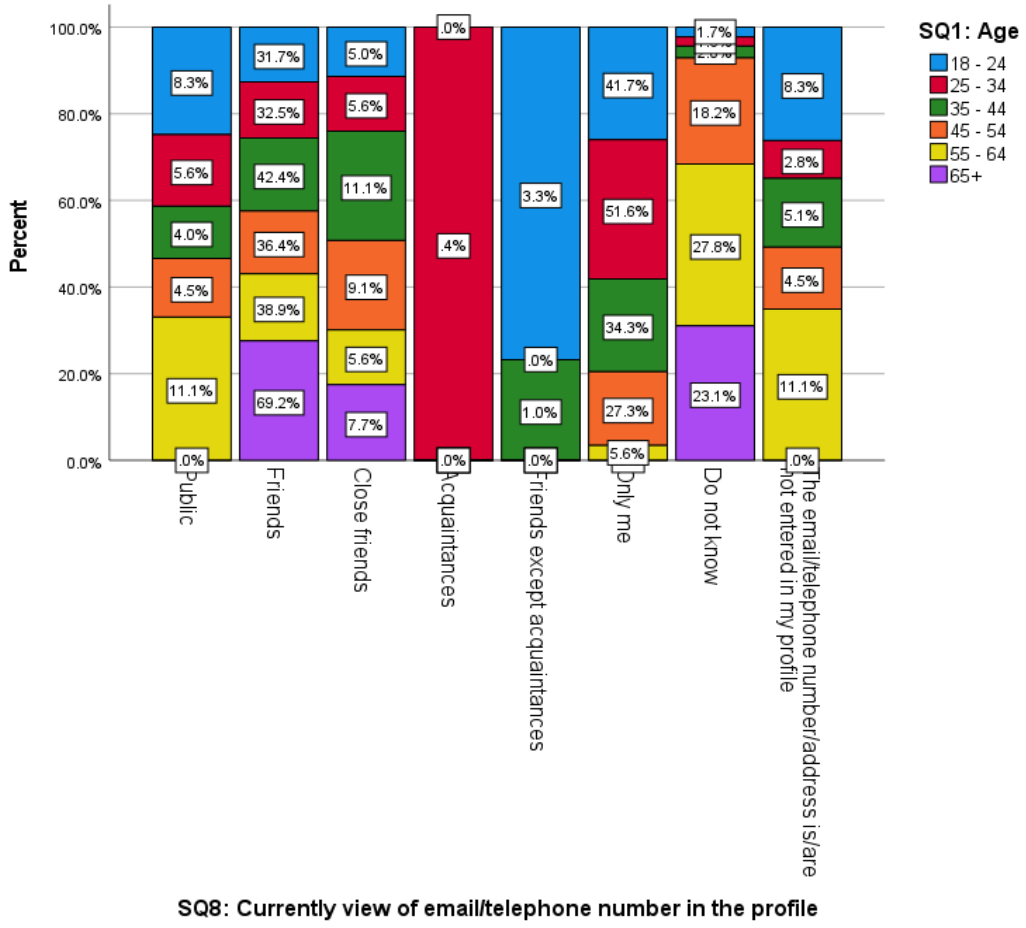


Figure C.13: Age-wise distribution related to the current view of/email/telephone number/address in Facebook profile

Only 5.1% males and 3.4% of females of total respondents are not vulnerable to cyber-attacks related to personal information disclosure as illustrated in Figure C.14.

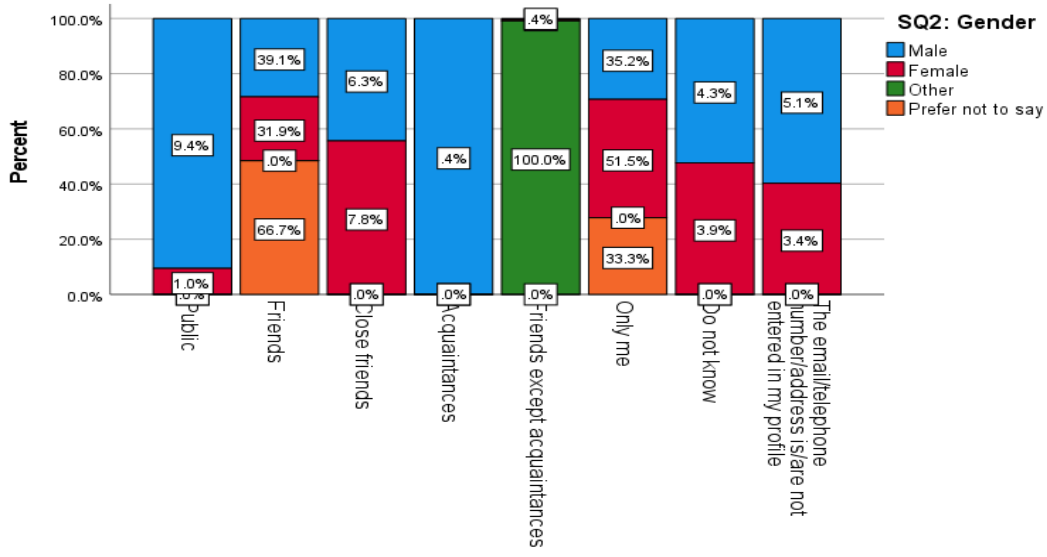


Figure C.14: Gender-wise distribution related to the current view of/email/telephone number/address in Facebook profile

Only 9.1% of certificate level holders, 6.6% of diploma level holders, 4.7% of bachelor's/graduate certificate or diploma level holders, and 5.2% of master's degree holders are not vulnerable from the cyber threats on disclosing personal details in Facebook profile as shown in Figure C.15.

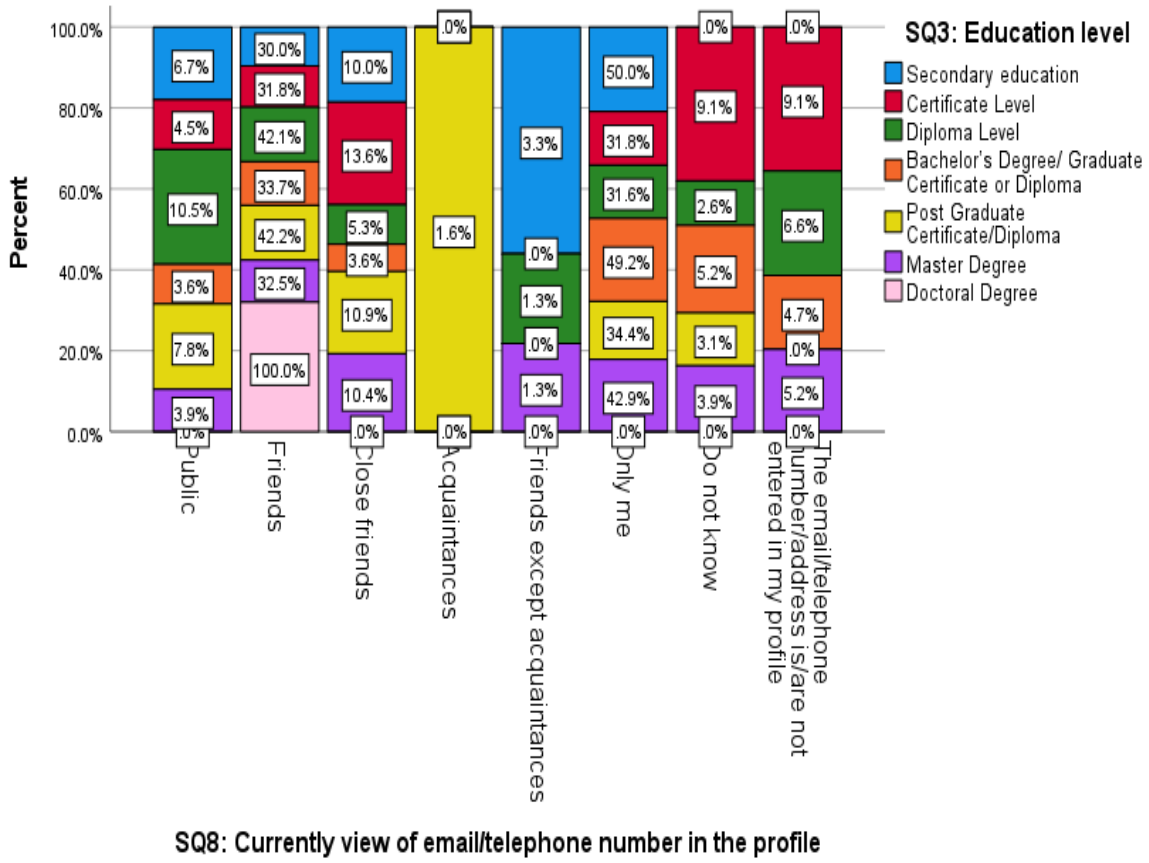


Figure C.15: Education level-wise distribution related to the current view of/email/telephone number/address in Facebook profile

Awareness of two-factor authentication in the Facebook platform is depicted in Figure C.16. Participant responses covering each age group representing at least moderate awareness can be explained as below.

- 18-24 – 58.4%
- 25-34 – 70.2%
- 35-44 – 60.7%
- 45-54 – 31.8%
- 55-64 – 22.2%
- 65+ - 23.1%

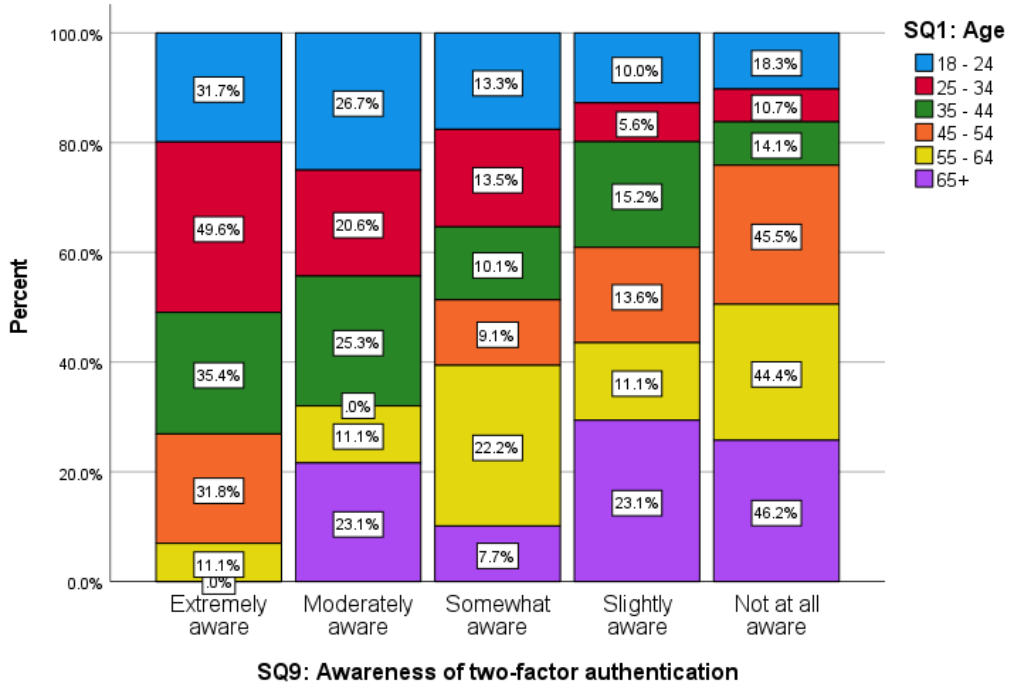


Figure C.16: Age-wise distribution related to awareness of two-factor authentication

Figure C.17 displays the gender-wise awareness of the two-factor authentication feature in Facebook. 68.4% of males, 52.9% of females, 100% of other category and 66.7% of prefer not to say category are at least moderately aware of the existence of this feature.

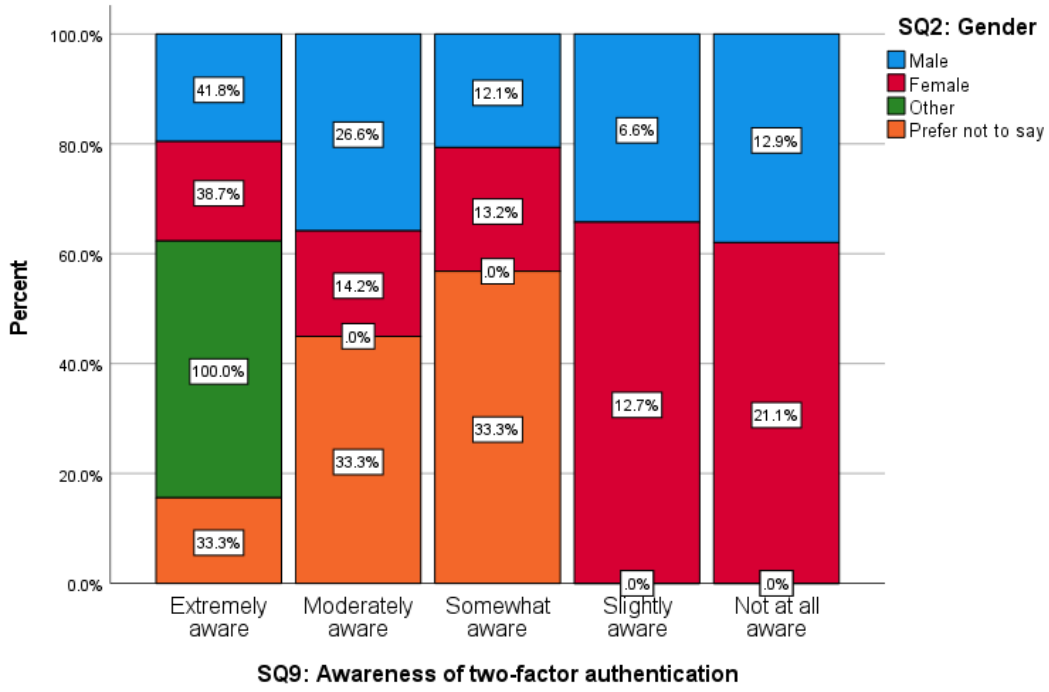


Figure C.17: Gender-wise distribution related to awareness of two-factor authentication

66.7% secondary education holders got at least moderate awareness on two-factor authentication feature while certificate holders, diploma holders, bachelor degree/graduate certificate or diploma holders, postgraduate certificate/diploma holders, and master's degree holders at least moderately aware on this representing 36.3%, 55.3%, 67.4%, 60.9%, and 61.1% respectively. Doctoral degree holders are either somewhat aware or slightly aware of this with 50% representation in each answer as shown in C.18.

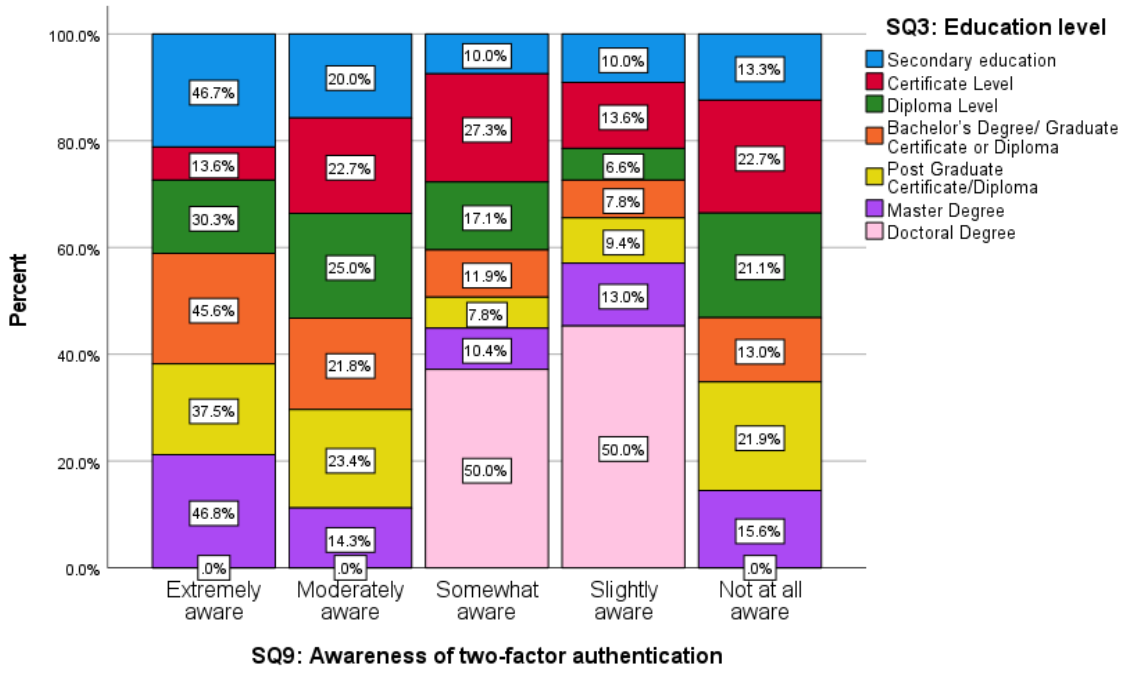


Figure C.18: Education level-wise distribution related to awareness of two-factor authentication

As depicted in C.19, more than 50% of each age group do not use the two-factor authentication feature in their Facebook account.

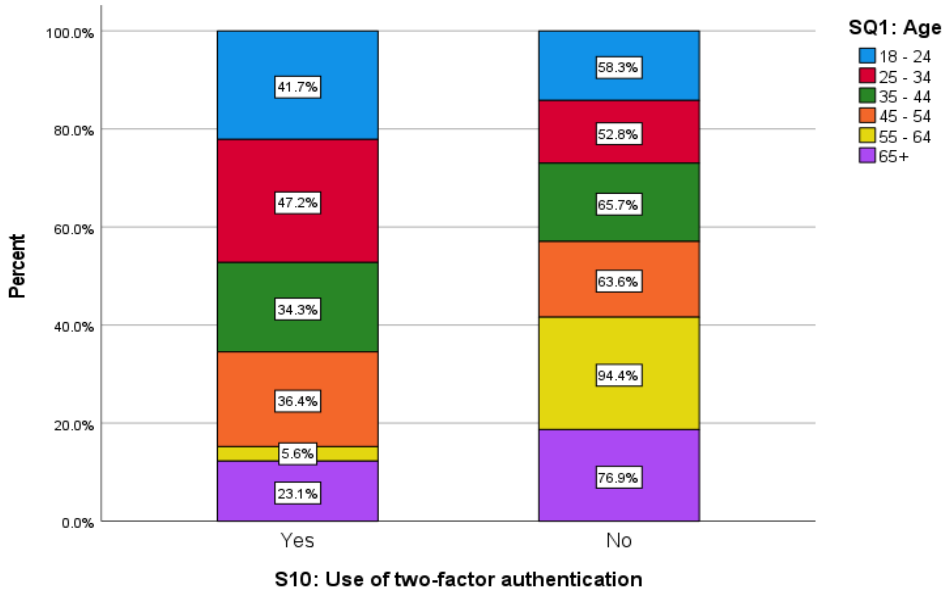


Figure C.19: Age-wise distribution related to use of two-factor authentication

Only 46.1% of males and 35.3% of females are using two-factor authentication in their Facebook profile making the rest of the respondents vulnerable to cyber-attacks in the platform as displayed in C.20.

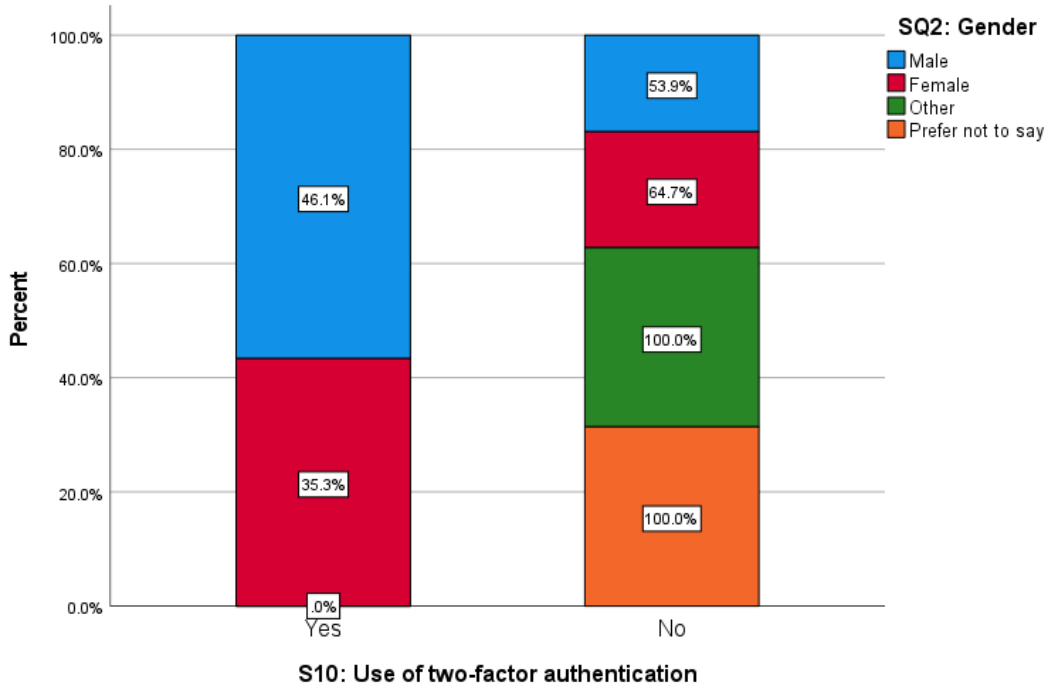


Figure C.20: Gender-wise distribution related to use of two-factor authentication

More than 50% of respondents in each education level are not using two-factor authentication in their Facebook profile as illustrated in Figure C.21.

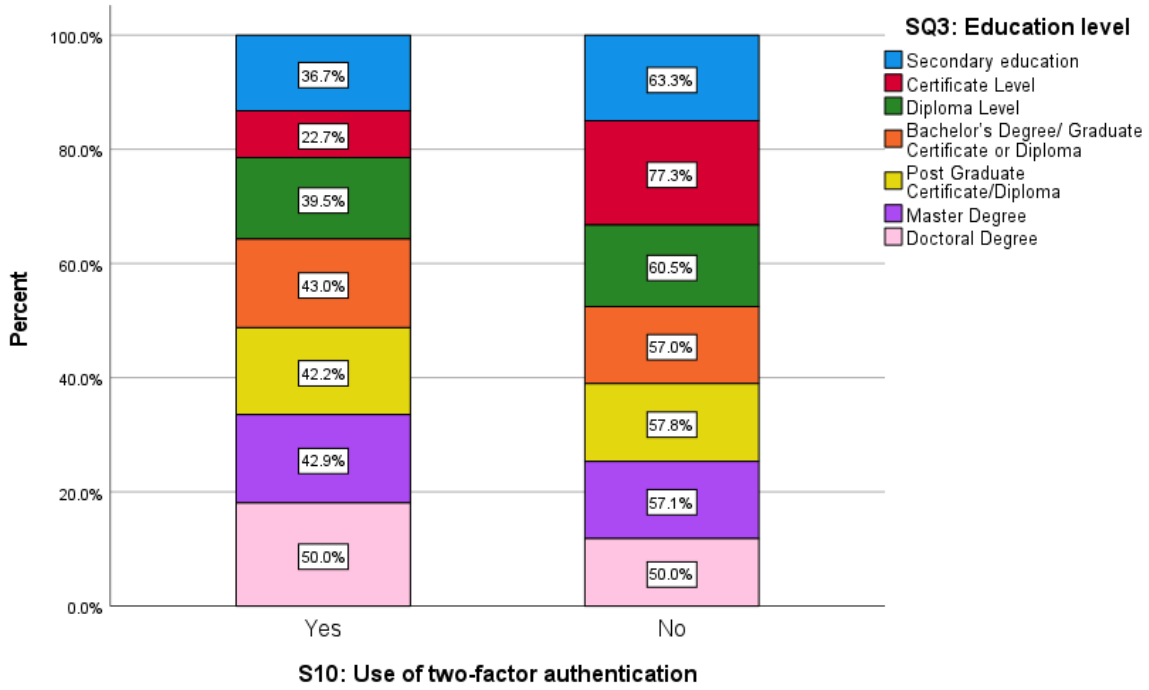


Figure C.21: Education level-wise distribution related to use of two-factor authentication

As illustrated in Figure C.22, 78.3% of survey participants from age 18-24, 27% of participants from age group 25-34, 61.6% participants from age group 35-44, 45.4% participants from age group 45-54, 27.8% participants from age group 55-64 and 30.8% participants from age 65+ are at least moderately aware of the Facebook feature that allows to set up who can send friend requests to their profile.

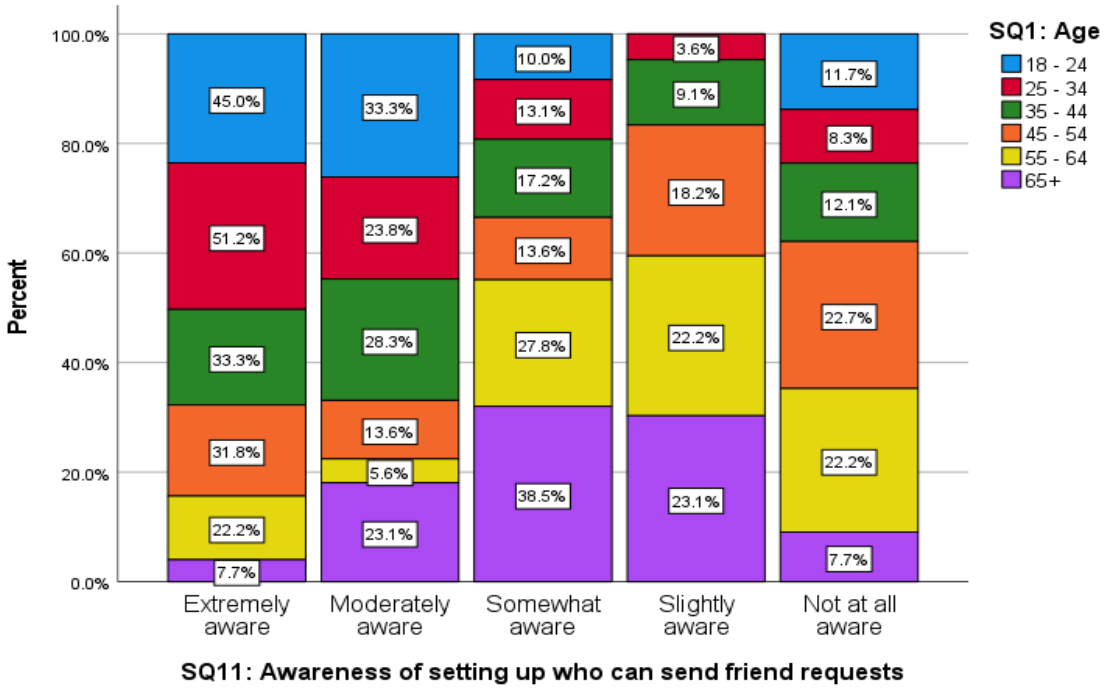


Figure C.22: Age-wise distribution related to awareness of setting up who can send friend requests

At least 69.5% of males, 66.1% of females, 100% of other, and 66.67% of prefer not to say categories are moderately aware of setting up who can send friend requests feature in the Facebook platform as shown in Figure C.23.

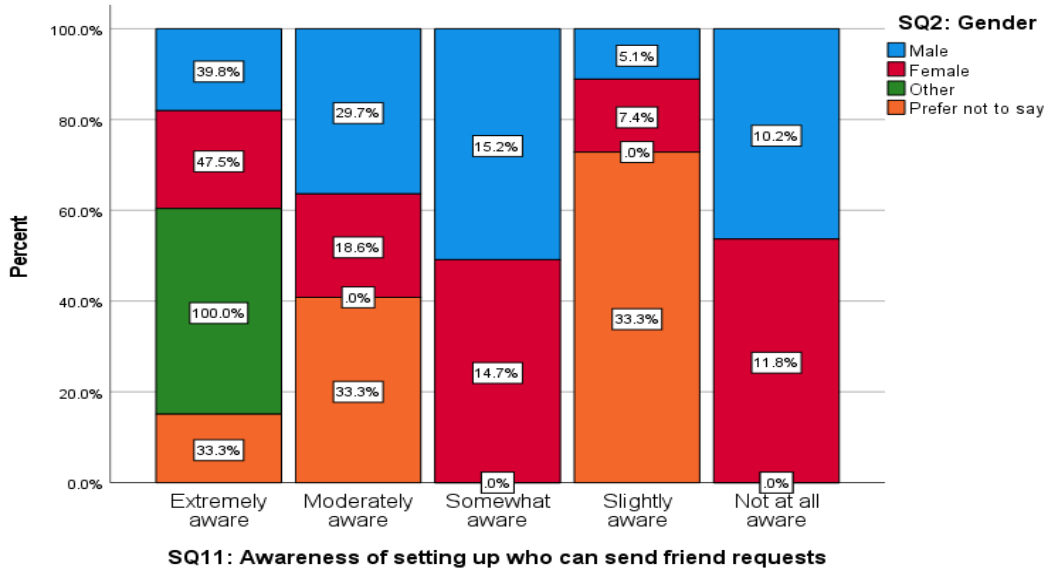


Figure C.23: Gender-wise distribution related to awareness of setting up who can send friend requests

As illustrated in Figure C.24, 76.7% of secondary education holders, 54.5% of certificate holders, 60.6% of diploma holders, 71.5% of bachelor's degree/graduate certificate or diploma holders, 62.5% of postgraduate certificate/diploma holders, 72.7% of master's degree holders and 50% of doctoral degree holders are at least moderately aware of the feature of setting up who can send friend requests to feature in Facebook.

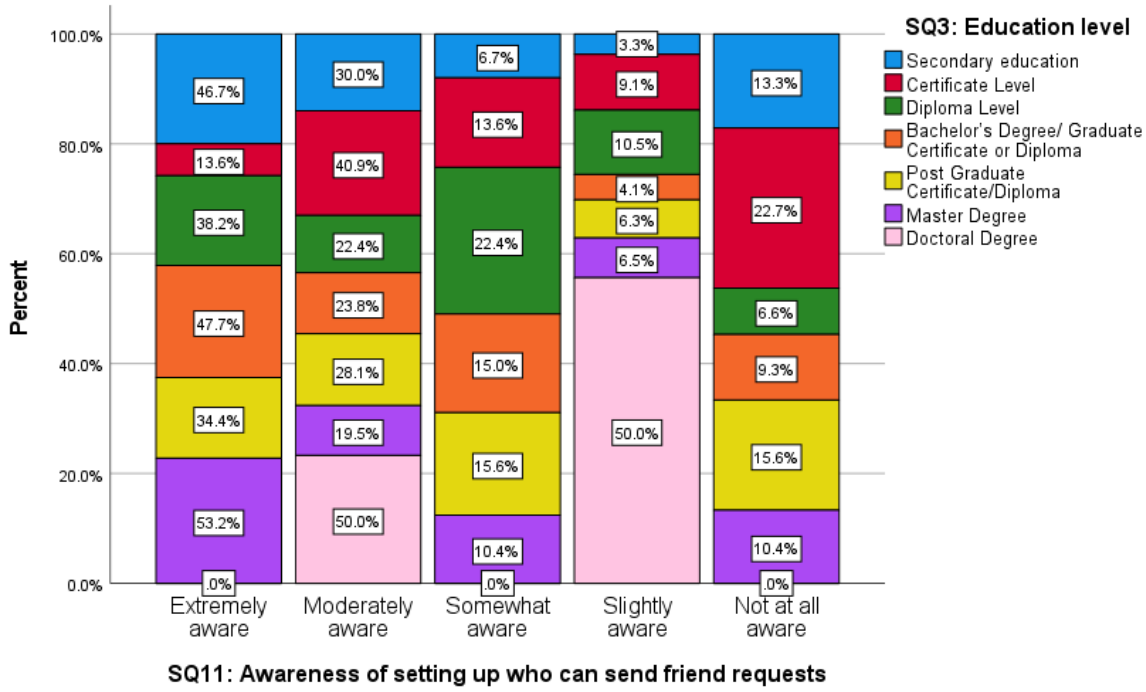


Figure C.24: Education level-wise distribution related to awareness of setting up who can send friend requests

77.8% of respondents from age 55-64 are not using setting up who can send friend requests option in Facebook making them the most vulnerable age group in this regard as displayed in Figure C.25. Subsequently, 69.2% of respondents in the age group 65+, 63.6% of respondents from age group 45-54, 56.7% of respondents in age group 18-24, 50.5% of the respondents in age group 35-44 and 41.3% respondents in the age group 25-34 are also not using setting up who can send friend requests option in Facebook. This makes the aforementioned respondents vulnerable to receive friend requests from unknown people.

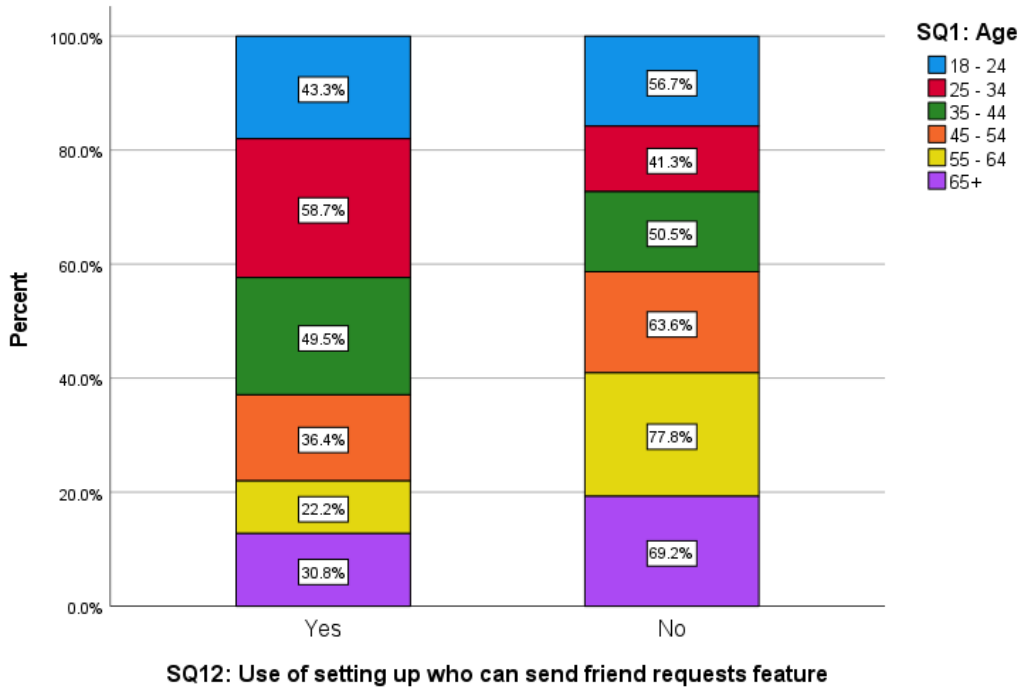


Figure C.25: Age-wise distribution related to use of setting up who can send friend requests

As per Figure C.26, 48% of males are using the setting up who send friend request feature and on the other hand, females represent 55.9% in this regard which is higher than males. 100% of other category uses this feature while only 33.33% of prefer not to say category uses this. All the other respondents are in the vulnerable category when considering this feature.

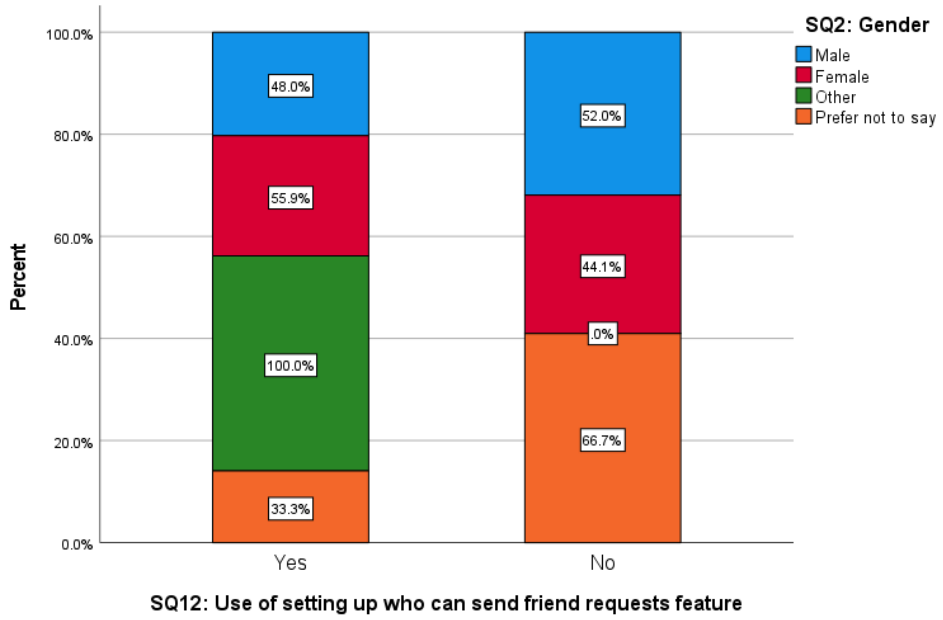


Figure C.26: Gender-wise distribution related to use of setting up who can send friend requests

More than 50% of respondents in secondary education, diploma level, bachelor's degree/graduate certificate or diploma, master's degree, and doctoral degree are using setting up who can send friend requests option in Facebook. However, certificate holders and postgraduate certificate/diploma holders use this option 40.9% and 46.9% respectively which is less than 50% as depicted in Figure C.27.

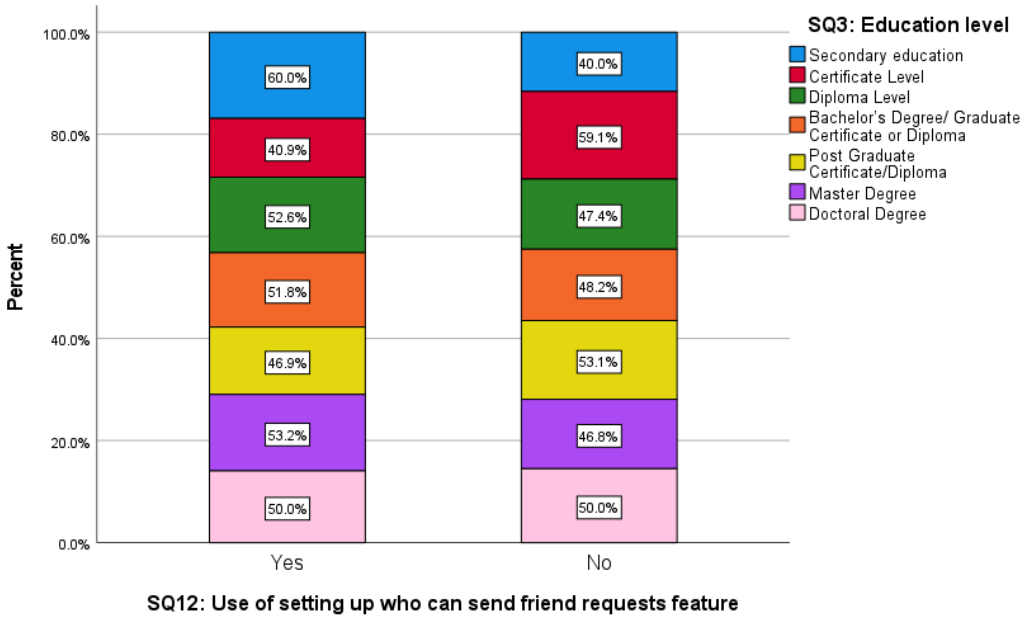


Figure C.27: Education level-wise distribution related to use of setting up who can send friend requests

Only 35% of the participants in the age group 18-24 are checking and updating privacy and security setting at least once a month on Facebook as displayed in Figure C.28. Statistics in this regard related to other age groups are 25-34: 25.4%, 35-44: 24.3%, 45-54: 4.5%, 54-64: 22.2% and 65+: 7.7% accordingly. That leads the rest of the remaining percentage in each age group to be the most vulnerable respondents to cyber threats in the Facebook platform as per survey results.

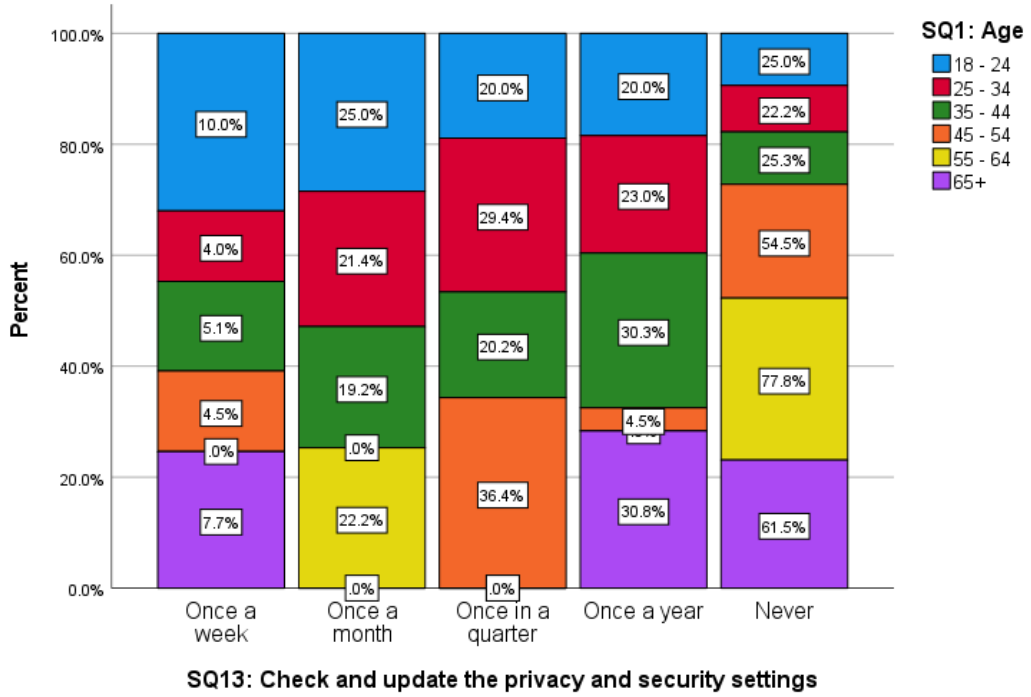


Figure C.28: Age-wise distribution related to check and update the privacy and security settings

As portrayed in Figure C.29, 25.4% of males and 24.5% of females are checking and updating Facebook privacy and security settings at least once a month. The rest of the respondents in male, female, other and prefer not to say categories are the most vulnerable to cyber threats in Facebook.

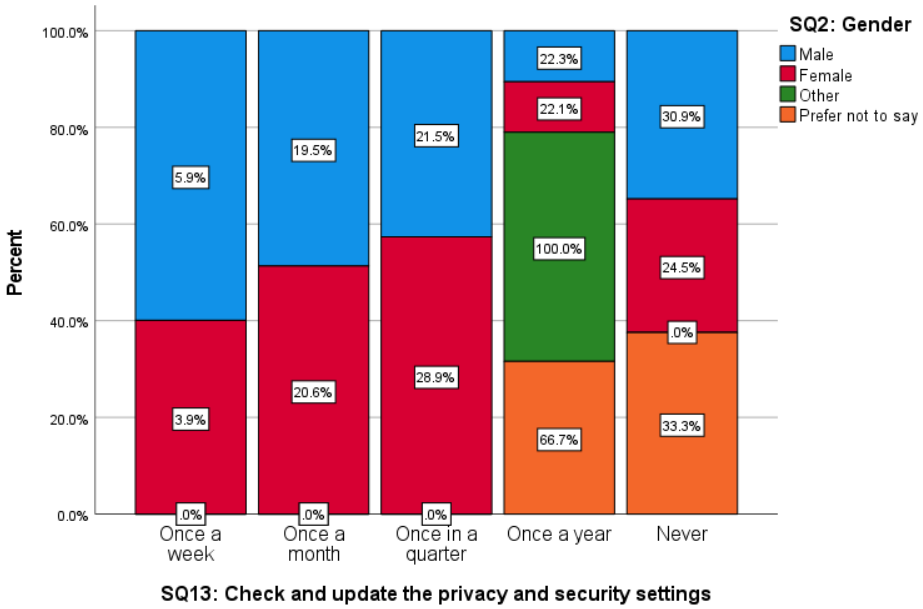


Figure C.29: Gender-wise distribution related to check and update the privacy and security settings

36.7% of secondary education holders, 27.3% of certificate holders, 25% of diploma holders, 25.9% bachelor's degree/graduate certificate or diploma holders, 21.9% of postgraduate certificate/diploma holders, and 19.5% of master's degree holders are at least checking and updating privacy and security setting in their Facebook accounts as displays in Figure C.30. Rest of the participants takes longer than that to check the privacy and security and that may lead them to become easy targets of cybercriminals in Facebook.

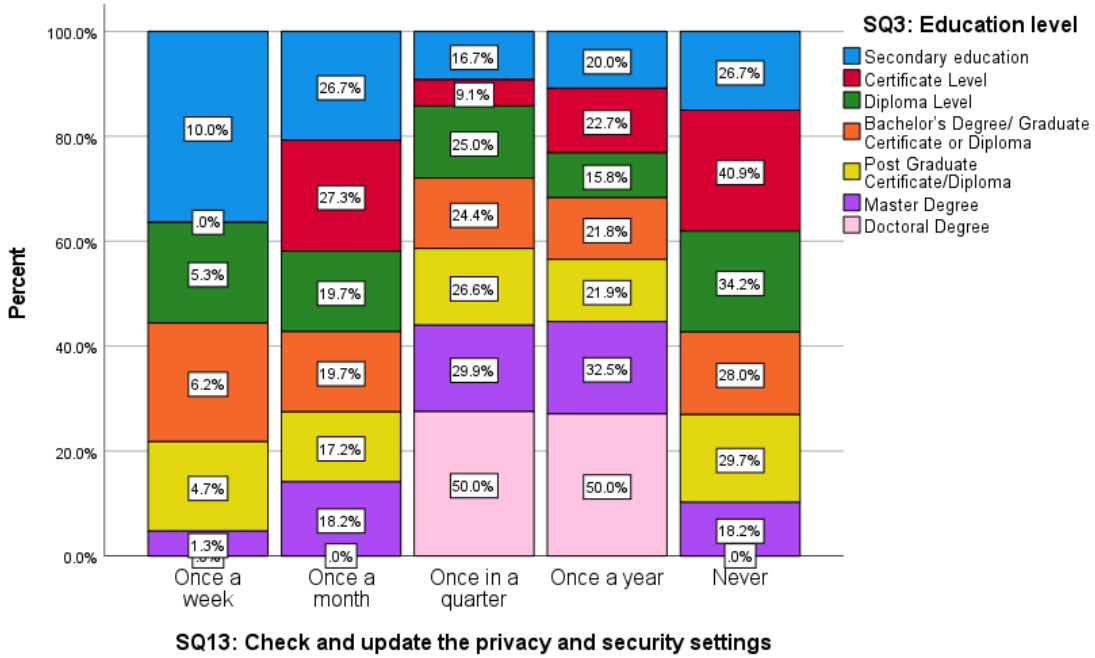


Figure C.30: Education level-wise distribution related to check and update the privacy and security settings

As per Figure C.31, 40% of participants in the 18-24 age group, 51.6% of participants in the age group 25-34, 66.7% of participants in the age group 35-44, 54.5% of participants in the age group 45-54, 33.3% of the participants in age 55-64 and 38.5% of participants in the age group 65+ are not vulnerable as they never accept a friend request from unknown people. According to these results, 35-44 is the most secured age group while 55-64 is the least secured age group in this regard. However, the rest of the participants are vulnerable in this matter since they accept a friend request from unknown people under any category representing rarely, sometimes, and always.

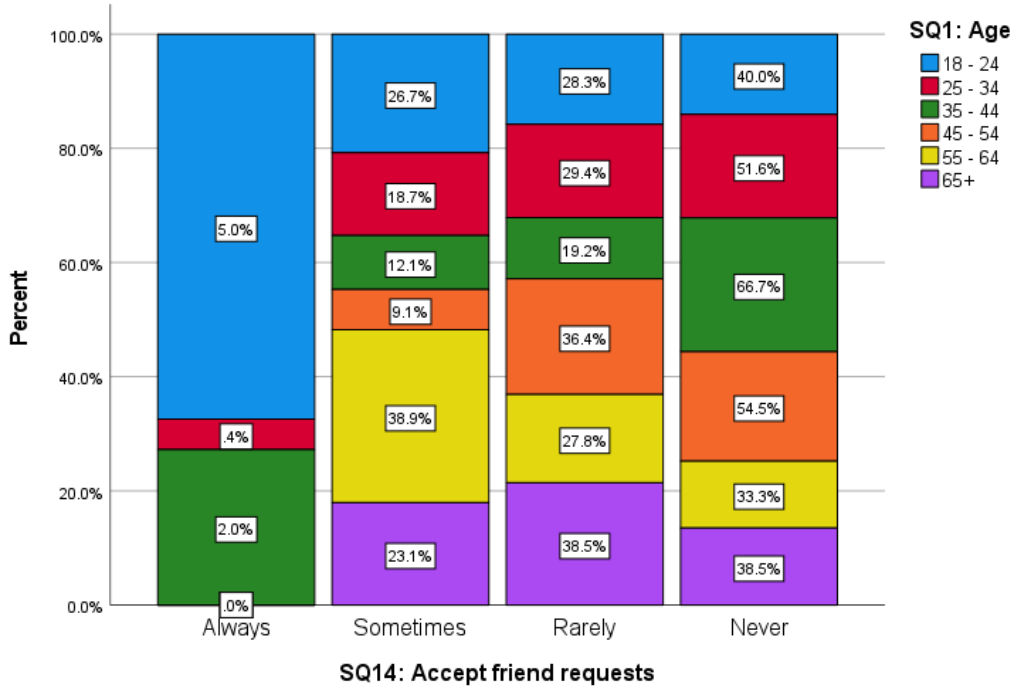


Figure C.31: Age-wise distribution related to accepting friend requests from unknown people

64.7% of females never accept friend requests from unknown people while only 42.2% of males do the same as depicted in Figure C.32. Also, 100% of other categories and 66.7% of prefer not to say category are not accepting friend requests from unknown people as well.

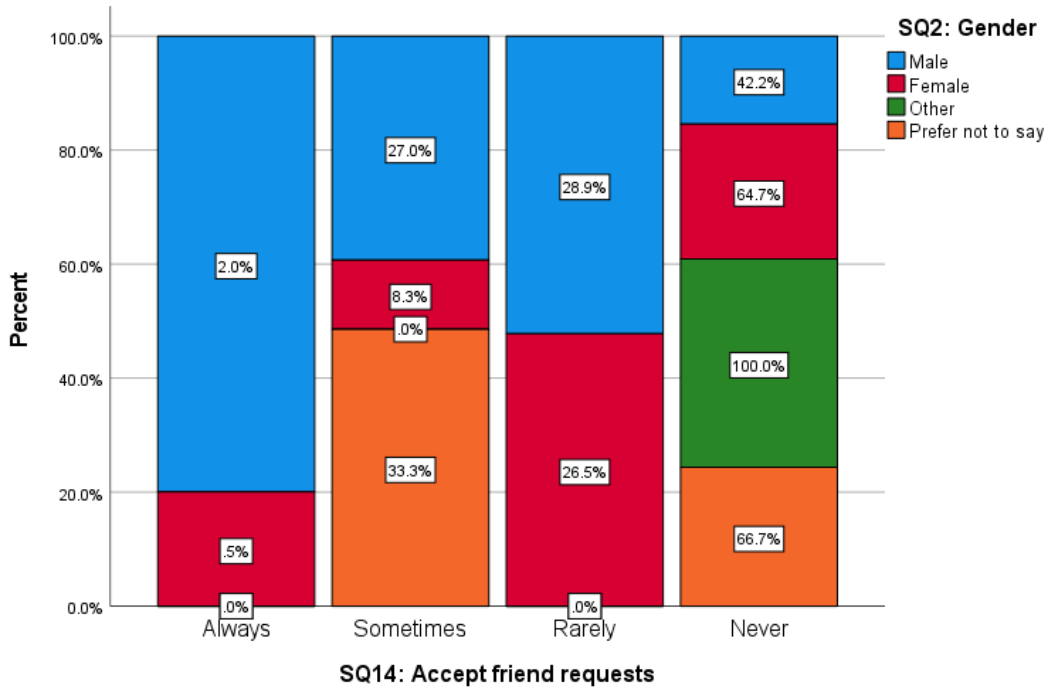


Figure C.32: Gender-wise distribution related to accepting friend requests from unknown people

More than 50% of respondents from certificate level, bachelor's degree/graduate certificate or diploma, postgraduate certificate/diploma, and master's degree holders never accept friend requests from unknown people as illustrated in Figure C.33. Percentage of secondary education holders and diploma holders who never accept friend requests from unknown people are 46.7% and 46.1% respectively. All the other respondents in each education level are vulnerable in this regard.

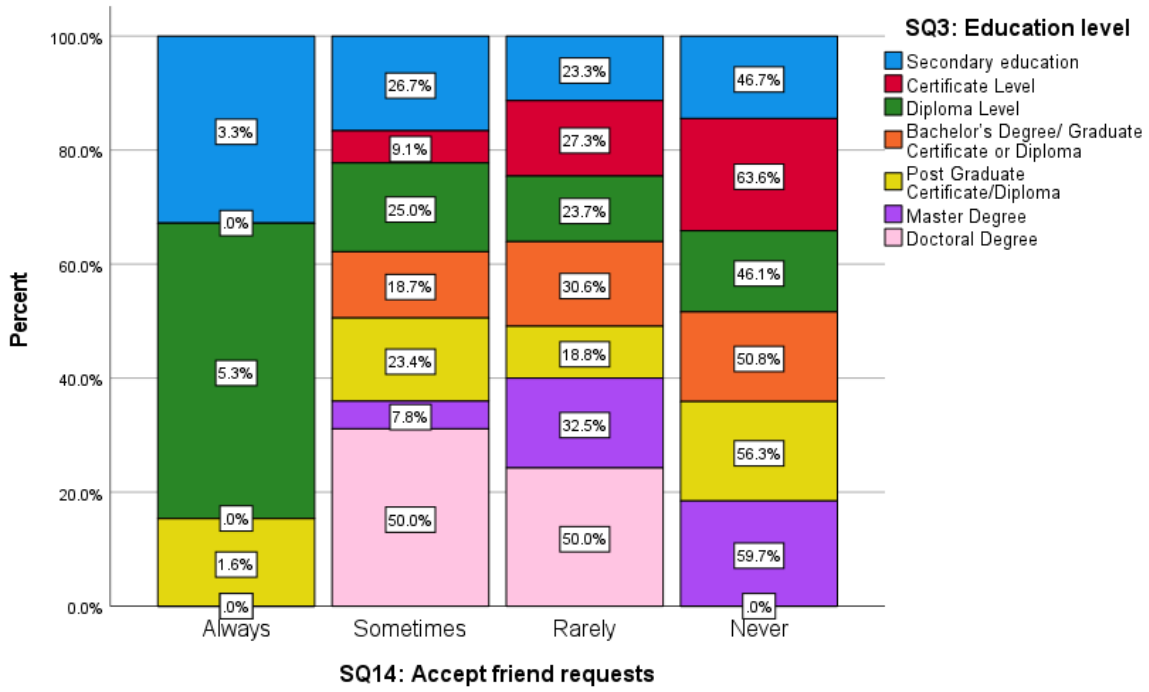


Figure C.33: Education level-wise distribution related to accepting friend requests from unknown people

As per Figure C.34, more than 70% of respondents from age groups 35-44, 45-54, and 55-64 never send friend requests to unknown people on Facebook. The percentage in this regard in other age groups are 18-24: 55%, 25-34: and 62.7%, and 65+: 46.2%. The rest of the respondents are sending friend requests to unknown people rarely, sometimes, or always and hence comparatively more vulnerable for cybercrimes.

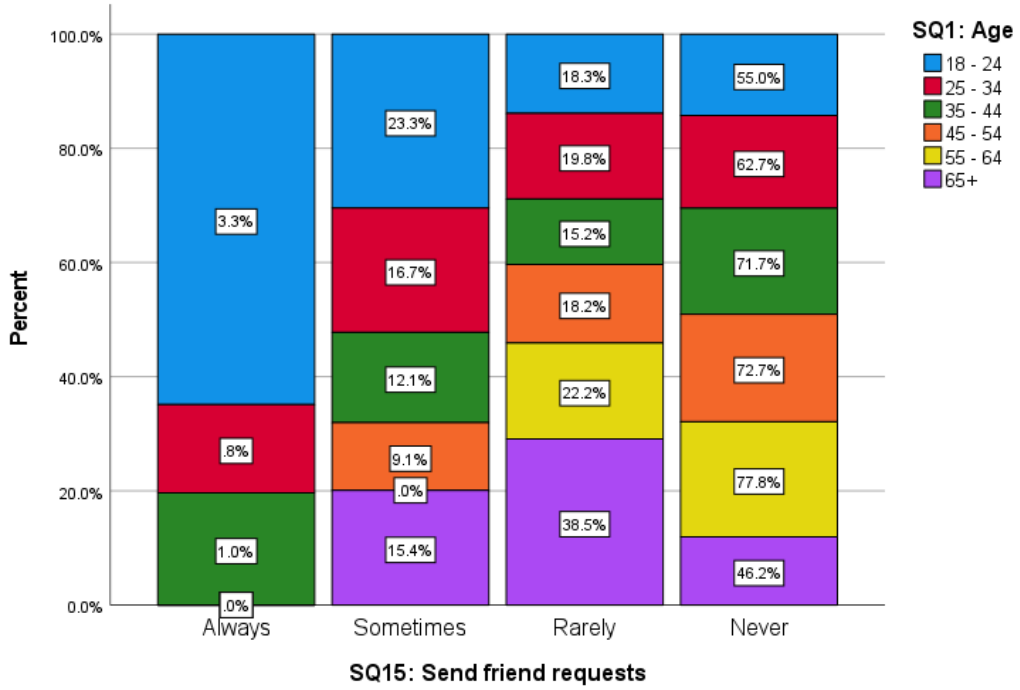


Figure C.34: Age-wise distribution related to sending friend requests to unknown people

84.8% of females never send friend requests to unknown people on Facebook while only 47.7% of males can do the same as per Figure C.35. 100% of prefer not to say category also never send friend requests to unknown people. All the other respondents are comparatively vulnerable to cybercrimes since they send friend requests to unknown people rarely, sometimes, or always.

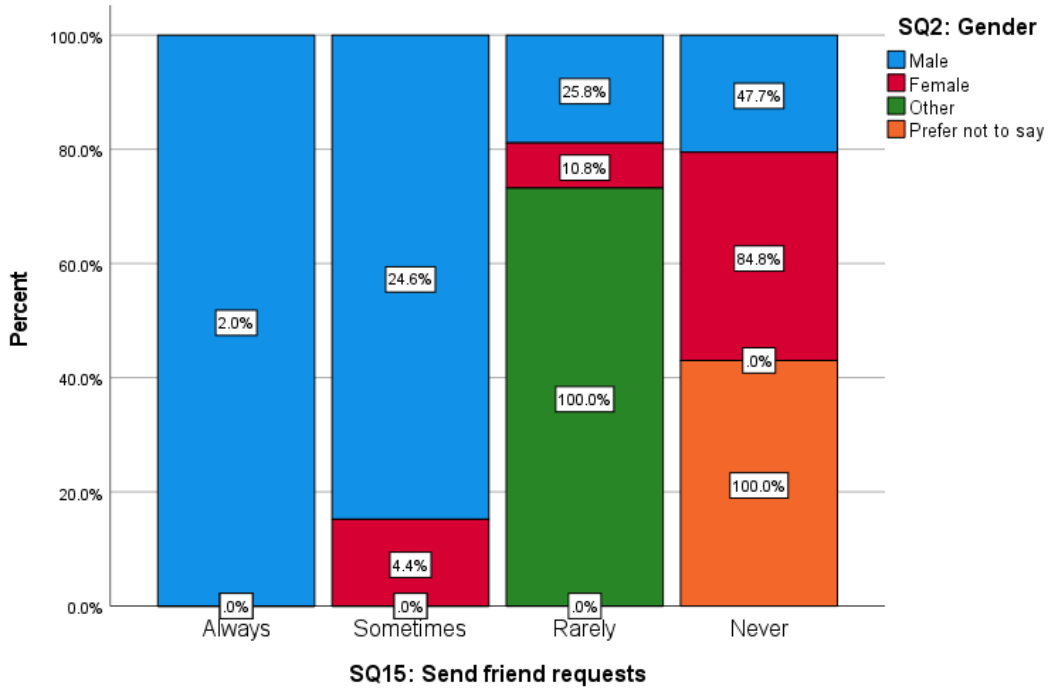


Figure C.35: Gender-wise distribution related to sending friend requests to unknown people

81.8% of certificate holders never send friend requests to unknown people on Face book representing the highest percentage from all education levels in this regard. Then 71.4% of master's degree holders, 70.3% of postgraduate certificate/diploma holders, 61.8% of diploma holders, 61.7% of bachelor's degree/graduate certificate or diploma holders, and 46.7% of secondary education holders never send friend requests to unknown people in Facebook consequently as depicted in Figure C.36. All the other respondents are comparatively vulnerable to cyber threats on Facebook since they rarely, sometimes, or always send friend requests to unknown people on Facebook.

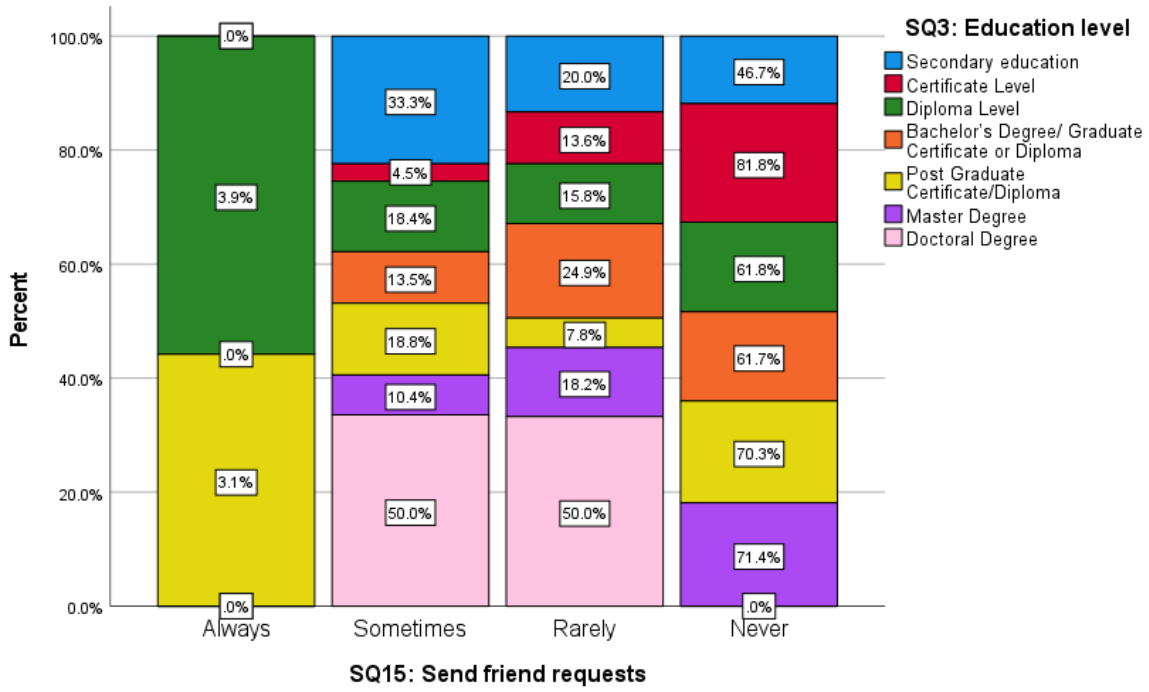


Figure C.36: Education level-wise distribution related to sending friend requests to unknown people

As per Figure C.37, 58.4% of respondents from age group 18-24, 71.1% of respondents from age group 25-34, 72.7% of respondents of age group 35-44, 59.1% of respondents of age group 45-54, 61.1% of respondents from age group 54-65 and 84.6% of respondents of the age group 65+ are unlikely to click unknown links sent to their profiles before verifying them. However, the rest of the respondents are comparatively vulnerable to cyber-attacks since they are either likely or neutral on clicking links sent by unknown people before verifying them.

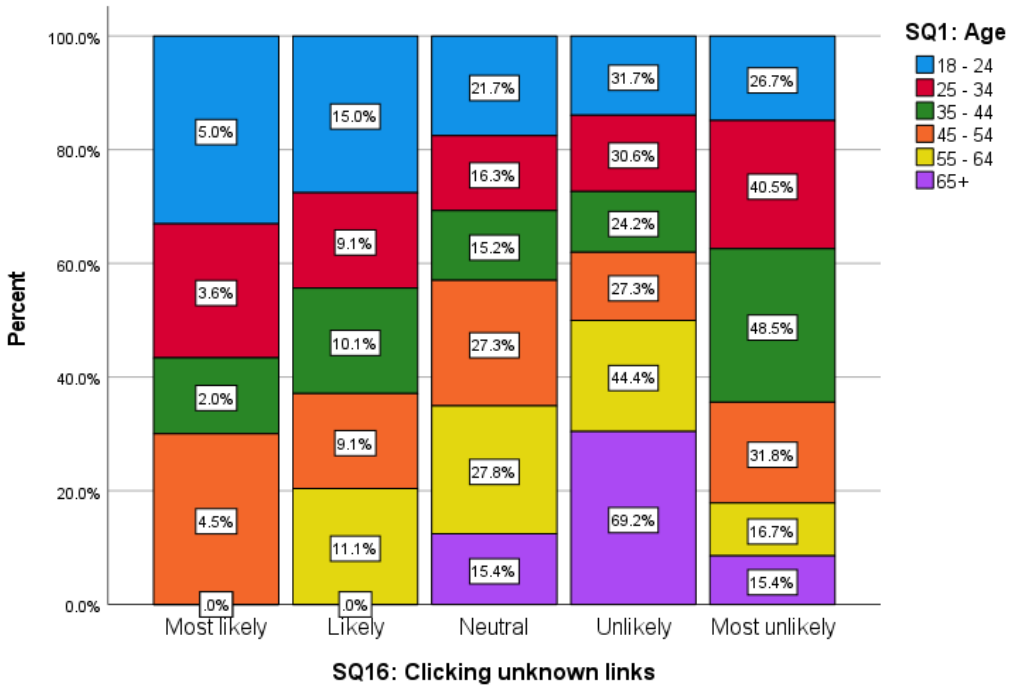


Figure C.37: Age-wise distribution related to clicking unknown links

66.8% of male respondents, 71.6% of female respondents, 100% of other and prefer not to say categories are unlikely to click the links sent by unknown people to their profiles before verifying them. All the other respondents are either likely or neutral in this regard and hence they are comparatively vulnerable to cyber-attacks.

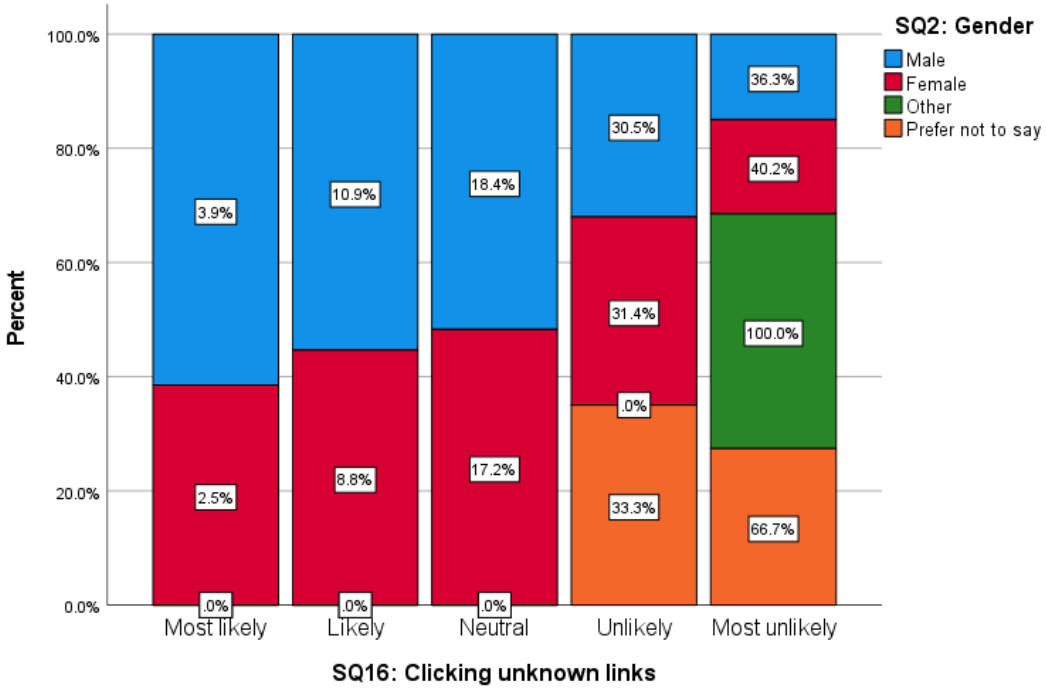


Figure C.38: Gender-wise distribution related to clicking unknown links

As portrayed in Figure C.39, 63.3% of secondary education holders, 63.7% of certificate holders, 55.3% of diploma holders, 77.2% of bachelor's degree/graduate certificate or diploma holders, 67.2% of postgraduate certificate/diploma holders, 68.9% of master's degree holders and 50% of doctoral degree holders are unlikely to click links sent by unknown people to their Facebook profile before verifying them. All the other respondents are either neutral or likely to click unknown links before verifying them and thereby vulnerable to cyber threats.

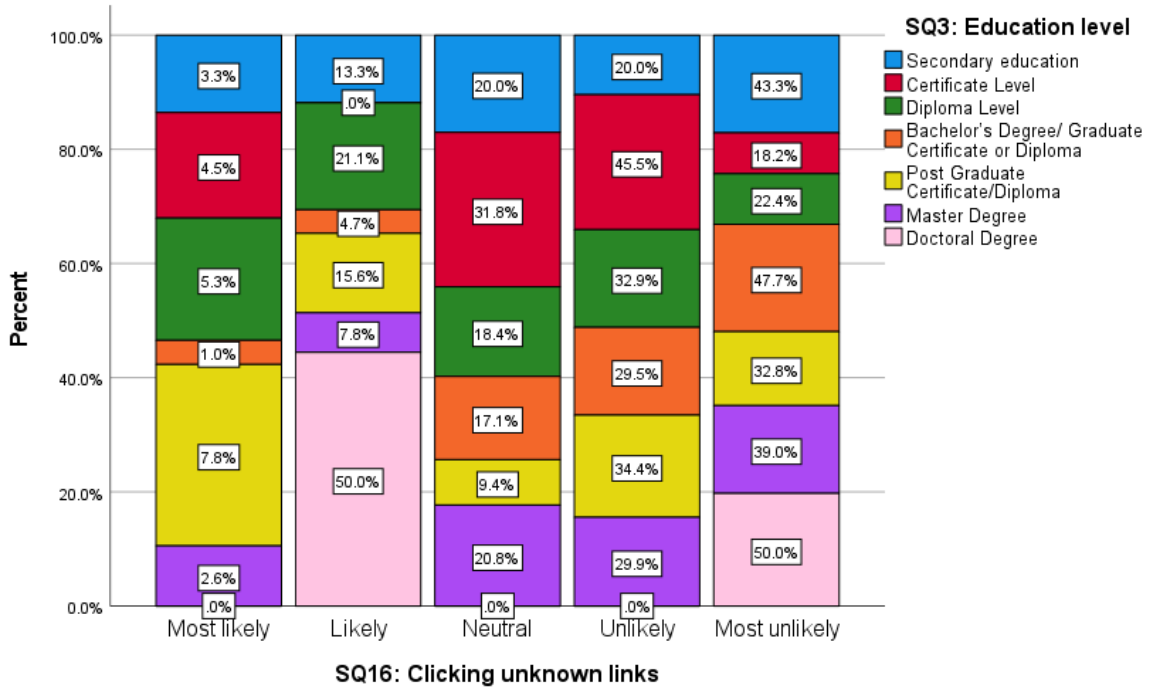


Figure C.39: Education level-wise distribution related to clicking unknown links

Only 18.3% of participants in the age group 18-24, 14.3% participants in the age group 25-34, 10.1% participants from age group 35-44, 27.2% of participants in the age group 45-54, and 5.6% participants in the age group 55-64 are changing their Facebook password at least once in a quarter as illustrated in Figure C.40. Rest of the respondents are comparatively vulnerable for cyber threats since they password change frequency is too long.

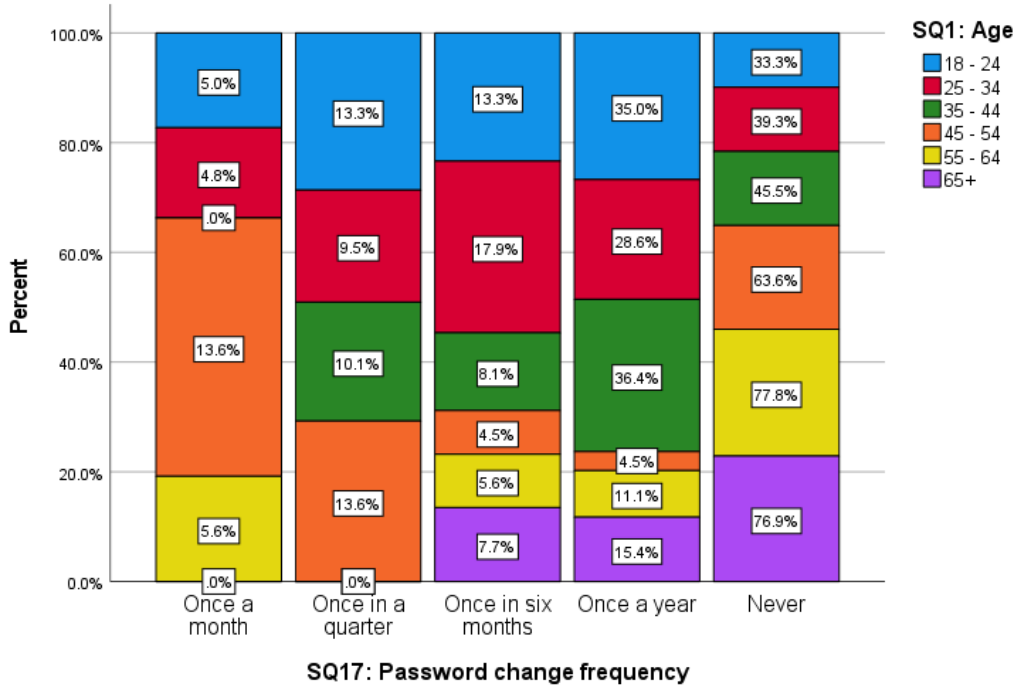


Figure C.40: Age-wise distribution related to changing password

16.4% of males and 10.7% of females are changing their Facebook password at least once in a quarter as displayed in Figure C.41. However, the majority of the respondents in all gender categories are comparatively vulnerable to cyber threats since their password change frequency is too long.

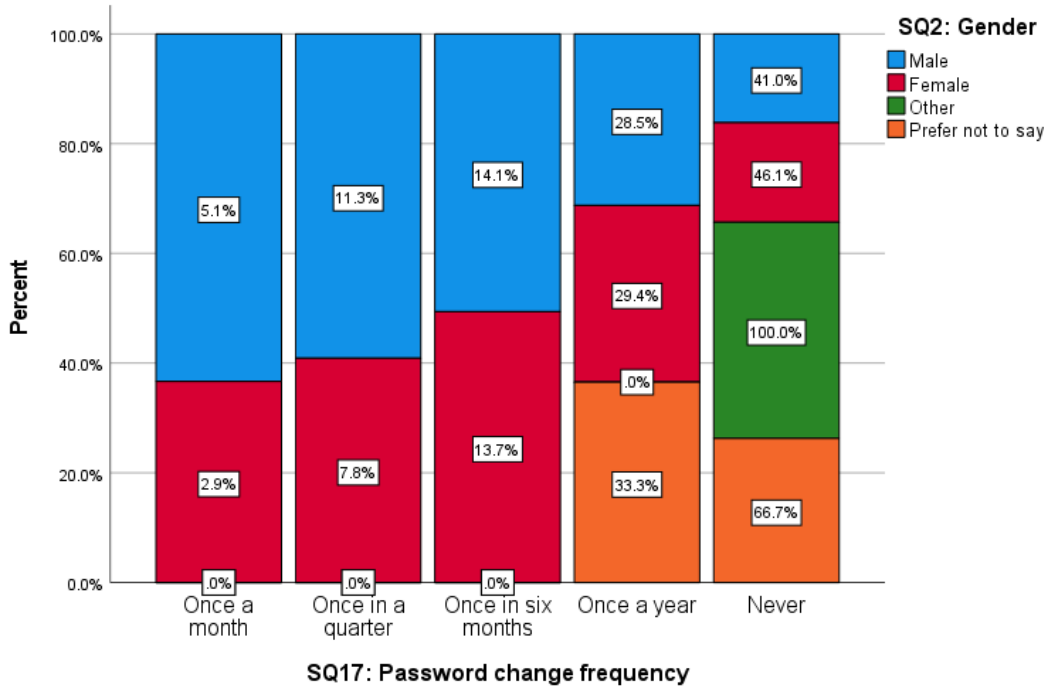


Figure C.41: Gender-wise distribution related to changing password

Figure C.42 illustrates that only 16.6% of secondary education holders, 4.5% of certificate holders, 13.2% of diploma holders, 15% of bachelor's degree/graduate certificate or diploma holders, 12.5% of postgraduate certificate/diploma holders, 13% of master's degree holders and 50% of doctoral degree holders are changing their Facebook password at least once in a quarter. All the other respondents are comparatively vulnerable to cyber threats since their password changing frequency is too long.

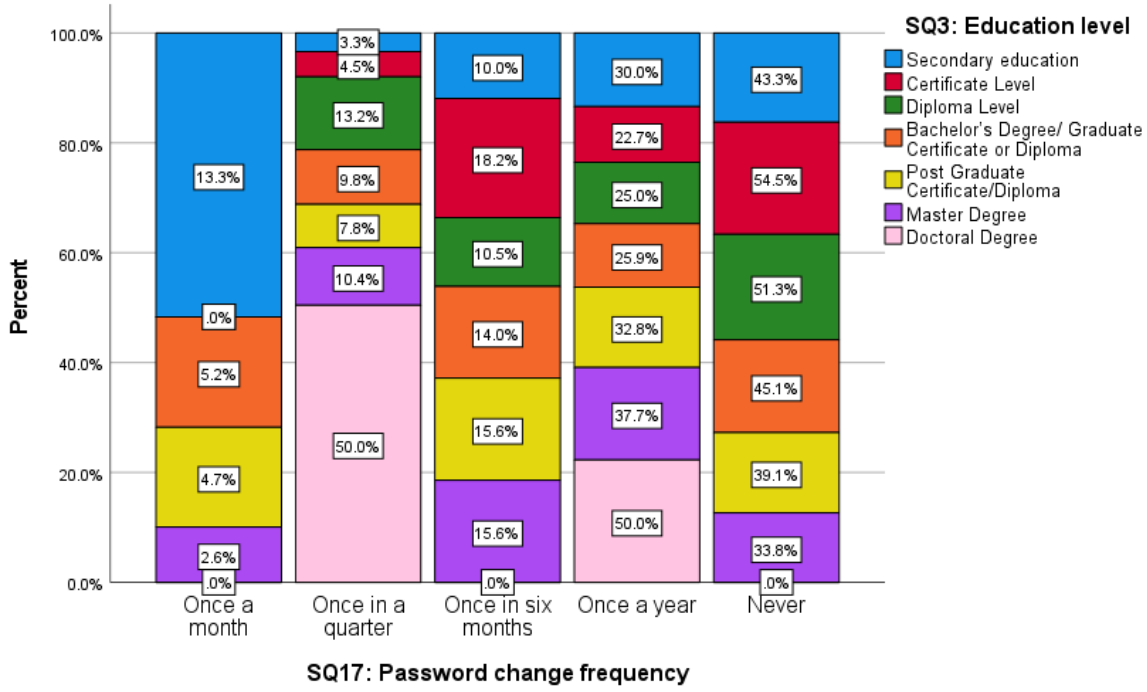


Figure C.42: Education level-wise distribution related to changing password

58.3% of respondents in the age group 18-24, 55.1% of respondents in the age group 25-34, 42.5% of respondents in the age group 35-44, 54.5% of respondents in the age group 45-54, 66.7% of respondents in the age group 55-64 and 38.5% of respondents in the age group 65+ are likely to logout from Facebook in any device that they no longer use it in that device. However, the rest of the respondents are comparatively vulnerable to cyber threats as they are either neutral or unlikely to do the same when using Facebook as depicted in Figure C.43.

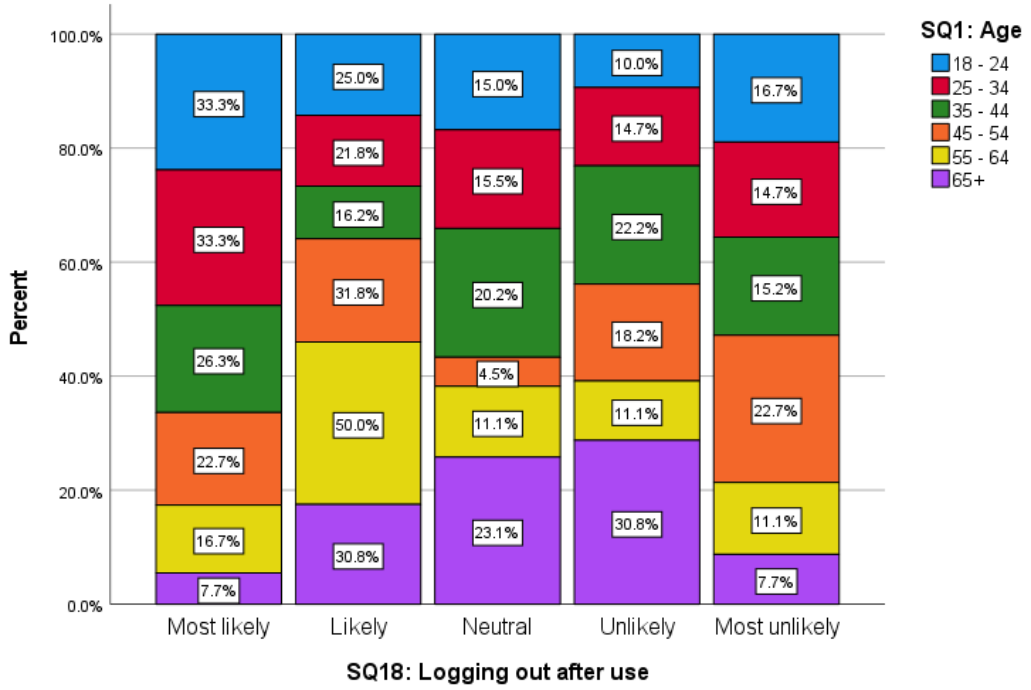


Figure C.43: Age-wise distribution related to logging out from any device after using Facebook

Figure C.44 portrays that 55.5% of male respondents, 49.5% of female respondents, and 66.7% prefer not to say respondents are likely to log out from Facebook from any device after they no longer use it in that device. All the other respondents are either neutral or unlikely about this and thereby comparatively vulnerable to cyber threats in Facebook.

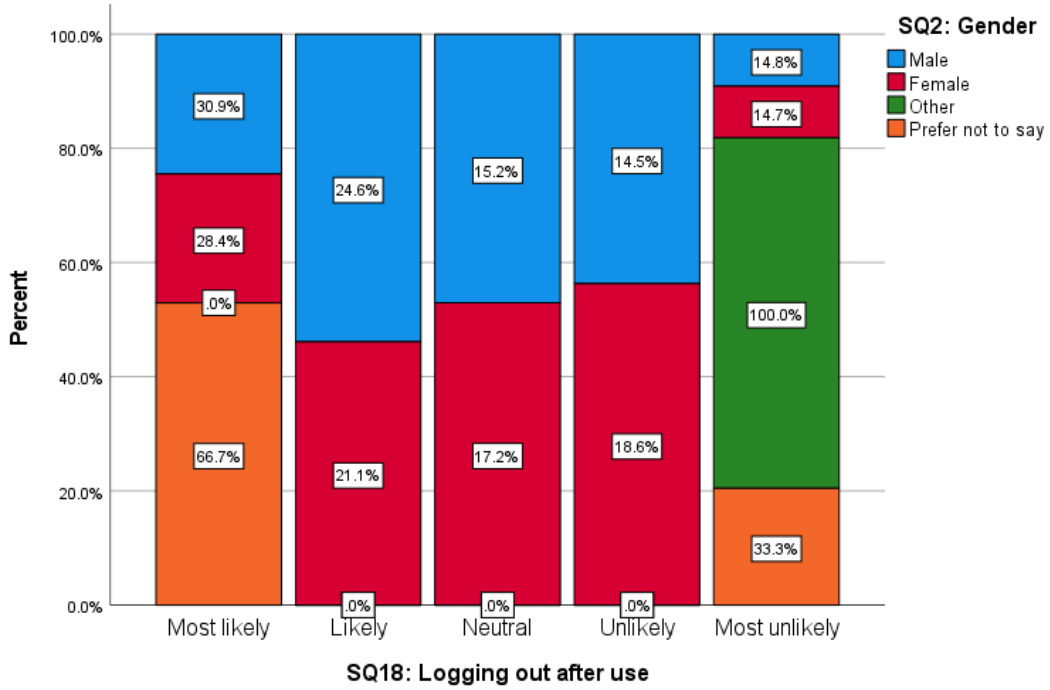


Figure C.44: Gender-wise distribution related to logging out from any device after using Facebook

63.4% of secondary education holders, 36.3% of certificate holders, 50% of diploma holders, 49.7% of bachelor's degree/graduate certificate or diploma holders, 59.3% of postgraduate certificate/diploma holders, 58.5% of master's degree holders, and 50% of doctoral degree holders are likely to log out from any device that they no longer use Facebook. On the other hand, all the other respondents are either neutral or unlikely to do and hence become comparatively vulnerable to cyber threats in Facebook as displays in Figure C.45.

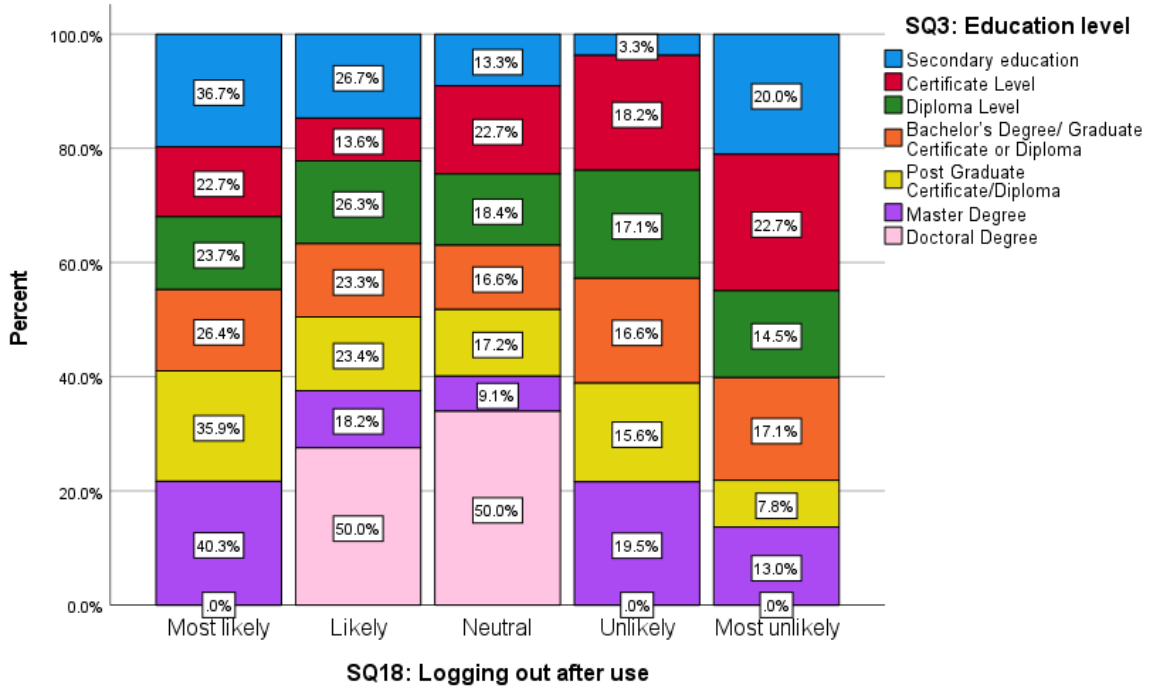


Figure C.45: Education level-wise distribution related to logging out from any device after using Facebook

As illustrated in Figure C.46, 78.3% of participants in the age group 18-24, 80.2% of participants in the age group 25-34, 76.8% of participants in age 35-44, 72.7% of participants in the age group 45-54, 61.1% participants in the age group 55-64 and 61.6% of participants in the age group 65+ consider security before sharing photos, videos, and posts in their Facebook profile. The rest of the participants are either neutral or unlikely to consider the security of photos, videos, and posts they share on Facebook.

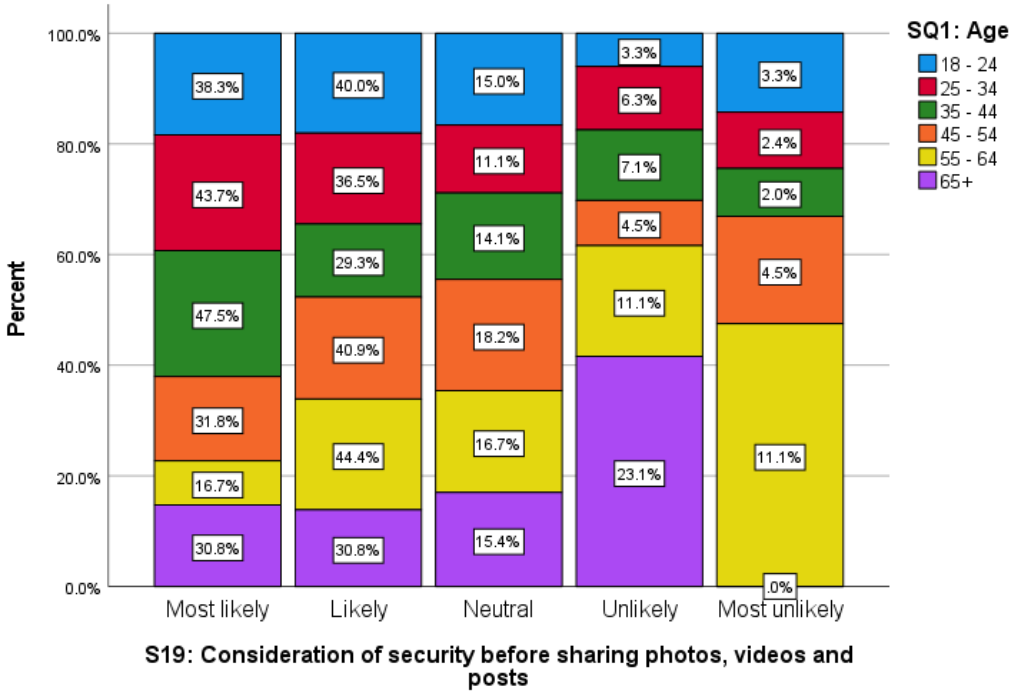


Figure C.46: Age-wise distribution related to considering security before sharing photos, videos, and photos

According to Figure C.47, 73.8% of males, 82.3% of females, and 100% of prefer not to say category at least likely consider security before sharing photos, videos, and posts on Facebook. All the other respondents are comparatively vulnerable to cyber threats on Facebook since they do not consider security before sharing photos, videos, and posts.

Figure C.47: Gender-wise distribution related to considering security before sharing photos, videos, and photos

83.3% of secondary education holders, 54.5% of certificate holders, 76.3% of diploma holders, 81.4% of bachelor's degree/ graduate certificate or diploma holders, 75.1% of postgraduate certificate/diploma holders, 76.7% of master's degree holders, and 50% of doctoral degree holders consider security before sharing photos, videos and posts in Facebook as depicted in Figure C.48. However all the other respondents in all education levels are vulnerable to cyber threats in Facebook since they do not consider security before sharing photos, videos, and posts.

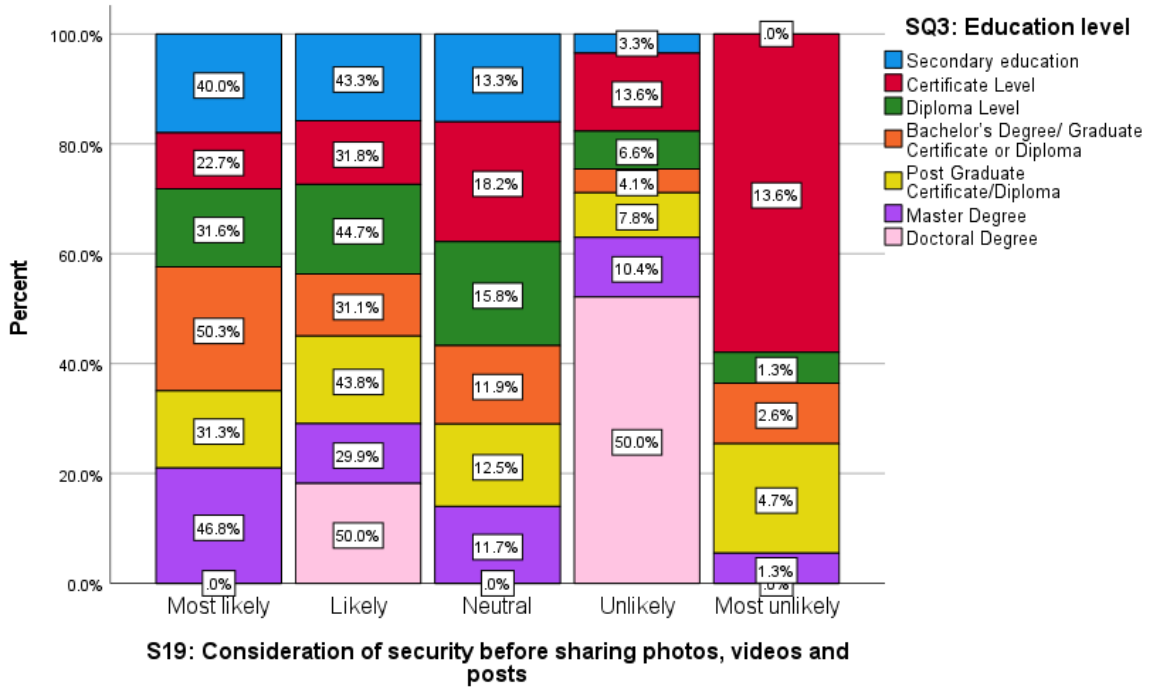


Figure C.48: Education level-wise distribution related to considering security before sharing photos, videos, and photos

As per Figure C.49, more than 80% of respondents in age groups 18-24 and 25-34 believe that they have at least a moderate level of awareness in Facebook while more than 70% of age groups 35-44, 45-54 and 55-64 believe they have at least moderate level awareness in Facebook. 69.2% of respondents in the age group 65+ believe that they have at least a moderate level of awareness as per survey results. The rest of the respondents either believed that they have a lower level of awareness or no awareness at all.

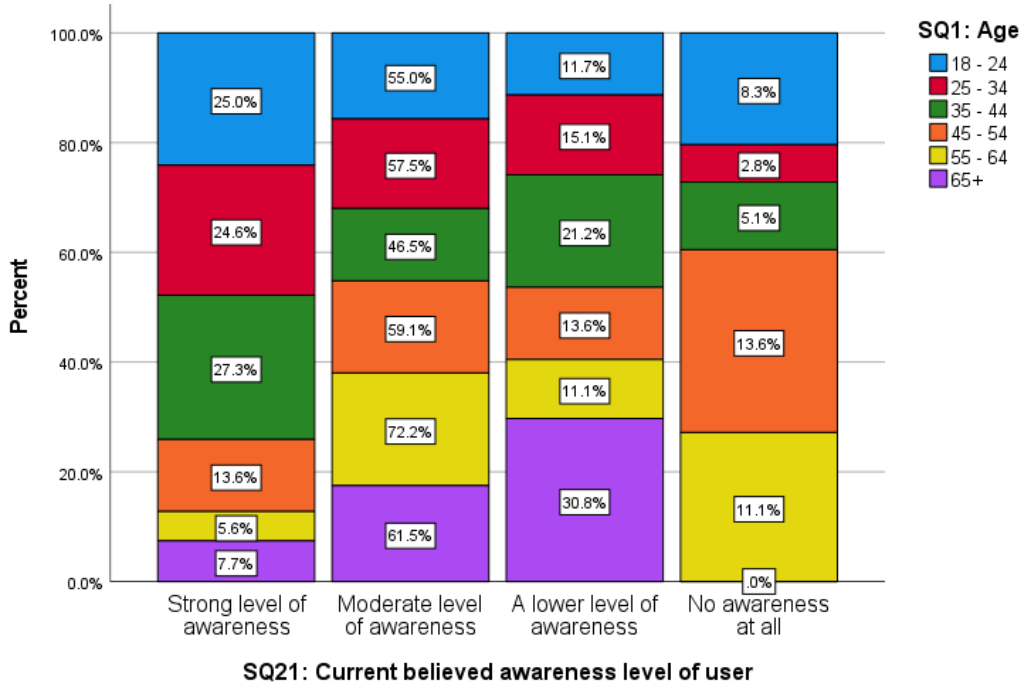


Figure C.49: Age-wise distribution related to current believed awareness level of Facebook users

According to Figure C.50 82.5% of males, 75% of females, 100% of other category, and 66.7% of prefer not to say category respondents believe that they have at least a moderate level of awareness in Facebook. Other respondents either believed that they have a lower level of awareness or no awareness at all.

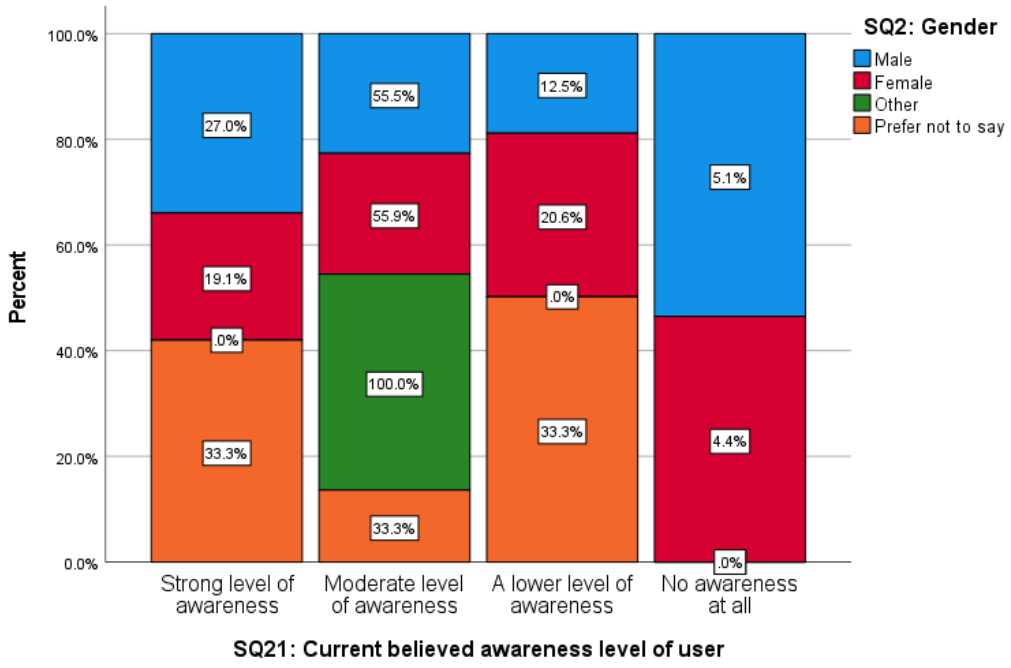


Figure C.50: Gender-wise distribution related to current believed awareness level of Facebook users

Figure C.51 shows that 80% of secondary education holders, 77.3% of certificate holders, 75% of diploma holders, and 80.8% of bachelor's degree/graduate certificate or diploma holders, 81.3% of postgraduate certificate/diploma holders, 77.9% of master's degree holders and 50% of doctoral degree holders believe that they have at least moderate level of awareness when using Facebook. The rest of the respondents either believed that they have a lower level of awareness or no awareness at all.

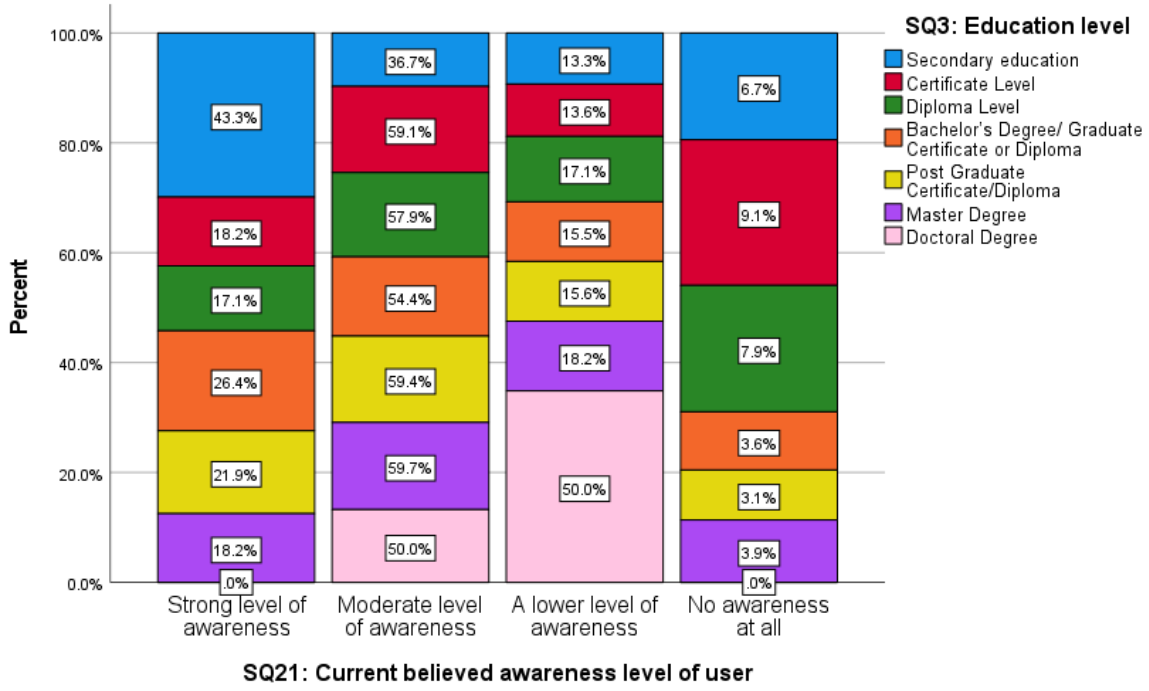


Figure C.51: Education level-wise distribution related to current believed awareness level of Facebook users

68.3% of respondents from age 18-24, 63.1% of respondents from age 25-34, 54.5% of respondents from age 35-44, 59.1% of respondents from age 45-54, 50% of respondents from age 55-64, and 38.5% of respondents from age 65+ are agreed upon believing that they have taken enough precautions to safeguard your Facebook profile from cyber threats as portrays in Figure C.52. The rest of the respondents neither agree nor disagree or disagree with this regard.

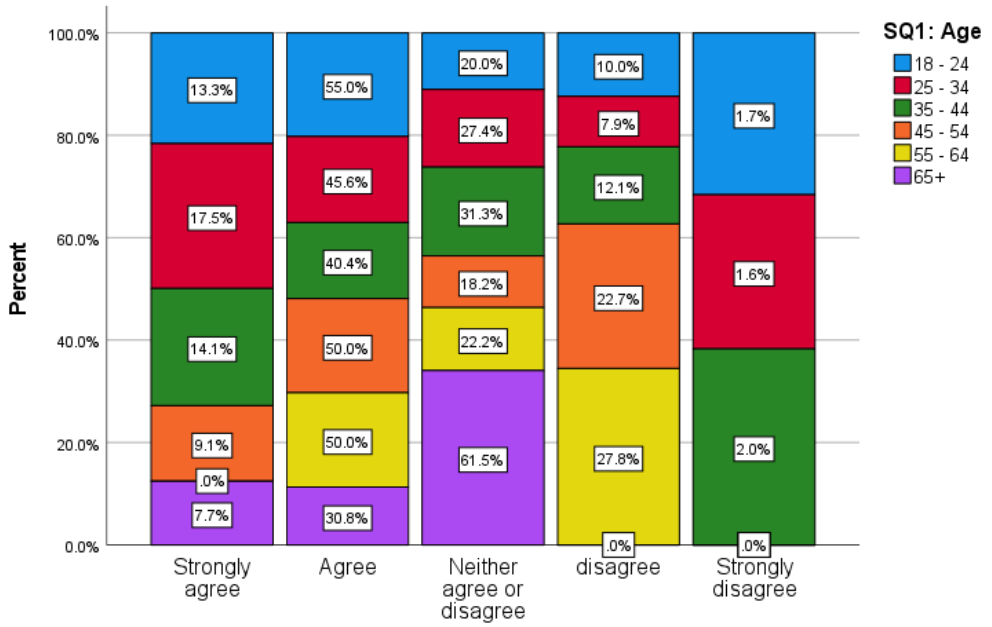


Figure C.52: Age-wise distribution related to the current believed behavioral level of Facebook users

According to Figure C.53, 60.6% of males, 59.8% of females, 100% of other and prefer not to say categories are agreed upon believing that they have taken enough precautions to safeguard your Facebook profile from cyber threats. The rest of the respondents neither agree nor disagree or disagree with this regard.

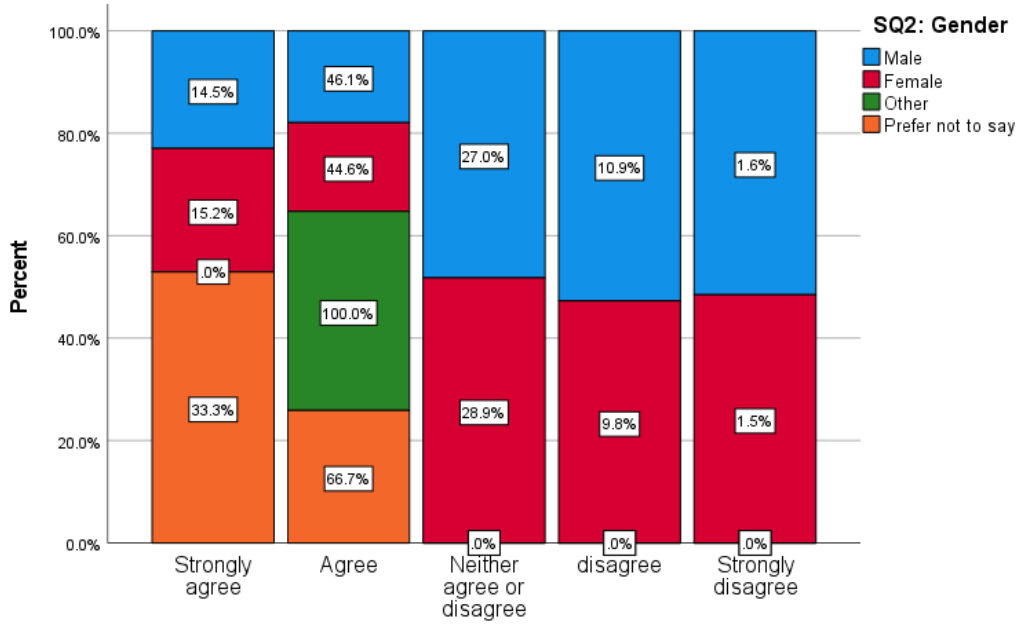


Figure C.53: Gender-wise distribution related to the current believed behavioral level of Facebook users

76.6% of secondary education holders, 59% of certificate holders, 60.6% of diploma holders, 62.2% of bachelor's degree/graduate certificate or diploma holders, 59.4% of postgraduate diploma holders, 52% of master's degree holders, and 50% of doctoral degree holders are agreeing upon believing that they have taken enough precautions to safeguard your Facebook profile from cyber threats as illustrated in Figure C.54. The rest of the respondents neither agree nor disagree or disagree with this regard.

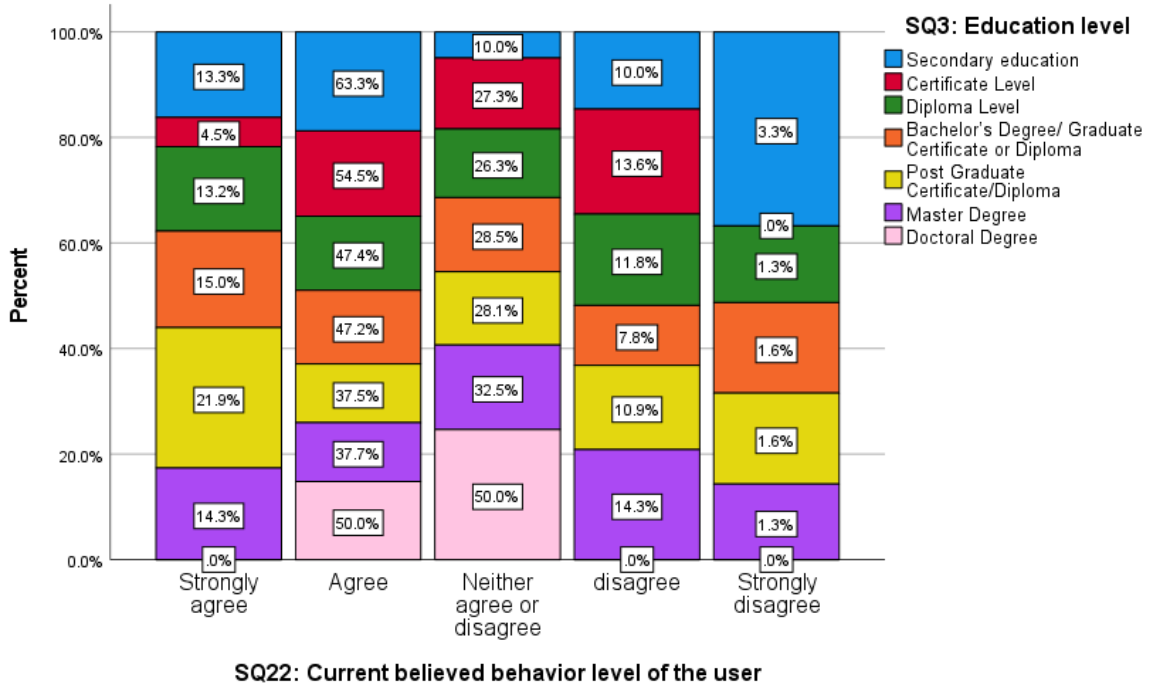


Figure C.54: Education level-wise distribution related to the current believed behavioral level of Facebook users

Appendix D-Ethics form

Wintec WAIKATO INSTITUTE OF TECHNOLOGY Te Kuratini o Waikato	**Research and Postgraduate Office (RPGO)** **Human Ethics in Research Group (HERG)**

LOW-RISK HUMAN ETHICS IN RESEARCH APPLICATION FORM

Please refer to the Ethics Guidelines prior to completing this application.

The RPGO is located at the City Campus, D-Block (Offices D2.22 – D2.24), email research@wintec.ac.nz or phone Megan Allardice on Ext. 3582 for more information.

Please see the last page of this document for detailed instructions for completing this form.

1.0 PROJECT TITLE	
	The recommended cybersecurity practices that can be followed by Facebook users to safeguard themselves from cyber threats when using the Facebook platform in the New Zealand context

2.0 RESEARCHER(S)		
2.1	Primary researcher's name	Thilini Bhagya Gothami Herath
2.2	School//Centre/Unit	Waikato Institute of Technology
2.3	Contact Details (Telephone and E-mail)	0284328407 thiher04@student.wintec.ac.nz
2.4	Is this application a:	☒ Student Application ☐ Staff Application
2.5	If this is a student application, please provide the Module code here	INFO901/2101
2.6	Is this project a staff application that utilizes work partially or wholly undertaken by students who are not participants (e.g. data collection undertaken by a researcher's class)?	N/A
2.7	If so, please clearly describe what the role of these students is to be in this research, what the work will be used for explicitly (including any issues regarding authorship of research outputs such as journal articles), and what steps have been taken to ensure students are aware of this.	N/A

2.8	Name of other Researcher(s) and positions. (If this is a student application please provide the name(s) of the project supervisor(s) and indicate that they are supervisors here.)	Dr. Monjur Ahmed Dr. Prashanth Khanna
2.9	Contact Details of other researchers and/or supervisors (Telephone and E-mail)	monjur.ahmed@wintec.ac.nz prashant.khanna@wintec.ac.nz
2.10	Is this application:	☒ A new application ☐ A subsequent approval request following a significant change to an already approved application

3.0 PROJECT TIMELINE

The projected start date for **data collection** *(once this ethics application is approved. Please note, projects can only begin once applications have been approved, regardless of the level of risk)*: 08th of March 2021

The projected end date: 18th of June 2021

4.0 PROJECT SUMMARY (please include your research purpose and objectives, the methodology will be dealt with in Section 6)

Facebook users become victims of cybercrimes every day although there is an internal security platform that exists within the Facebook platform. Therefore the users should take necessary precautions to protect themselves from users' points of view as well. Hence this research proposal is mainly focused on forming research on identifying the recommended cybersecurity practices for Facebook users in the New Zealand context followed by the post-positivist research methodology.

There are three main objectives of this research. The first one is to identify the current awareness and practices of Facebook users in terms of securing their privacy and personal data in their profiles. The second objective is to identify the vulnerability level of Facebook users based on their responses. The third objective is to recommend best practices to overcome the identified vulnerability level and safeguard their privacy and user data from any misuse.

5.0 PROJECT METHODOLOGY (including methods for data collection)

A statistically significant online survey will be used to collect the data under the quantitative method when conducting the research. The sample size is 600 (Source: survey systems calculator, 2020.) which is calculated based on the 3.568 million New Zealand Facebook user population at level 4 confidence interval along with confidence level 95%. The responses will be collected based on the convenience sampling method.

6.0 CONSIDERATION OF ETHICAL ISSUES AND PROCESSES

Please describe below the process that you have undergone to discuss and analyze the ethical issues present in this project. (For example, who have you consulted in regards to ethical issues or in completing the screening questionnaire and this Low-Risk application)

Below ethical considerations will be addressed throughout the research processes thoroughly.

Risk of Harm

All the survey questions are general and not at all likely to cause any distress to the respondents at any point. Also, the research has been designed to treat people equally without any discrimination. Please see the statistically significant survey questions in appendix 2 for further clarification.

Informed and voluntary consent

There is a sentence on the first page of the online survey asking the respondent for their consent to proceed with the survey. They can either continue or leave the survey at any point. To the best of the researcher's knowledge, it is assumed that all respondents can issue valid consent. Also, the respondents are asked to continue the survey only if they are above age 18, currently use the Facebook platform, and currently live in New Zealand. Please refer to the participant information sheet in appendix 4 and screening questions in appendix1 for more details.

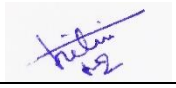
Privacy and confidentiality

No personal and/or sensitive data will be collected during the online survey in a way that a particular individual can be identified. Please refer to the statistically significant survey questions in appendix 2 for further clarification.

Conflict of interest

No particular group will be targeted including Wintec students or staff for this research purpose. Also, participants will not be known to the researcher at any point.

Researcher(s) signature(s) (the <u>name and signature</u> of all researcher(s) are to be included):

Name	Signature	Date
Thilini Bhagya Gothami Herath		25/02/2021

Research Leader's signature:

Name	Signature	Date

Primary Supervisor's signature (if this is a student application):

Name	Signature	Date
Dr. Monjur Ahmed		

HERG Chairperson or delegated representative's signature (RPGO use only):

Name	Signature	Date

COMPLETING THIS FORM

Please note: A low-risk research project is one in which the nature of the potential/actual risk of harm to participants or the researcher is minimal and no more than is normally encountered in daily life. If, as a staff member, you are new to research or are in any doubt as to which application to submit, please consult with your Research Leader. If you are a student, your supervisor will be able to give you advice. If you are still in any doubt, don't hesitate to consult the RPGO.

Specific Instructions

- All questions are to be answered. Note the questions within require a mix of descriptions, yes/no answers and cross the box (**Double-click on checkboxes with your mouse and select 'Checked' from the options under 'Default Value'**).
- Research Leaders need to review the information in this form and sign it off prior to the application being made to the RPGO.
- Please forward one signed original copy to the RPGO, together with an electronic version to research@wintec.ac.nz.
- Low-Risk Human Ethics in Research Applications also need to be accompanied by a copy of the Information Sheet, Consent Form, and any Questionnaires or Interview Schedules for consideration. If Questionnaires/ Schedules are not yet confirmed, please supply the latest draft.
- No questions are to be deleted, even those that you feel you are not required to answer.
- No part of the research requiring ethical approval should commence prior to approval being confirmed.
- Applicants will receive official confirmation of submission via email from the RPGO once all conditions of this form have been completed.
- If you want to apply for an extension on a previously approved project, please contact the RPGO, as you will probably not need to submit a separate application.
- Applicants will be advised of the outcome of their application to the Human Ethics in Research Committee **no later than ten working days** after the completed and confirmed submission of this application.

HUMAN ETHICS IN RESEARCH LOW RISK APPLICATION FORM – CHECKLIST	
Research project title:	The recommended cybersecurity practices that can be followed by Facebook users to safeguard themselves from cyber threats when using the Facebook platform in the New Zealand context
Name of primary researcher:	Thilini Bhagya Gothami Herath

Attached please find (as applicable) in the order listed below	
Completed HERG Low-Risk Application Form	☒ Yes ☐ No

Consent Form for participants	☐ Yes ☒ No
Information Sheet for participants	☒ Yes ☐ No
Copy of Focus Group Questions, Interview Schedule, or similar	☒ Yes ☐ No